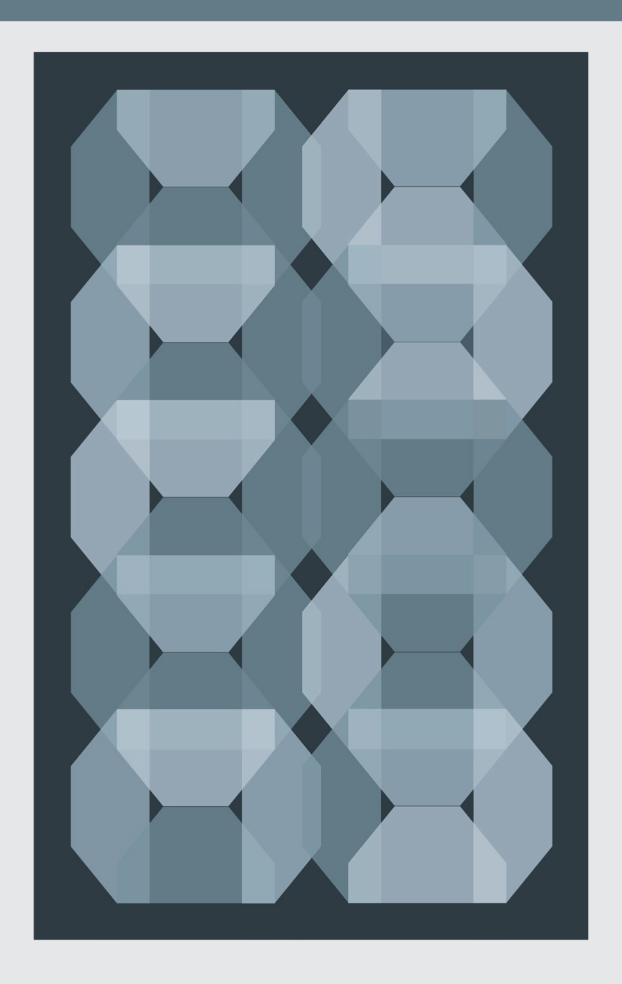
عالم المعرفة
سلسلة كتب ثقافية شهرية يصدرها
المجلس الوطني للثقافة والفنون والآداب - الكويت



المنطقة المعتمة:

التاريخ السري للحرب السيبرانية

تأليف: فرِدْ كابلان
ترجمة: لؤي عبدالمجيد




المجلس الوطني
للثقافة والفنون والآداب



Withe

عالم المعرفة
سلسلة كتب ثقافية شهرية يصدرها
المجلس الوطني للثقافة والفنون والآداب - الكويت

صدرت السلسلة في يناير 1978
أسسها أحمد مشاري العدواني (1923-1990) ود. فؤاد زكريا (1927-2010)

المنطقة المعتمة:

التاريخ السري للحرب السيبرانية

تأليف: فرِدْ كابلان
ترجمة: لؤي عبدالمجيد



مارس 2019
470



سلسلة شهرية يصدرها
المجلس الوطني للثقافة
والفنون والآداب

ترسل الاقتراحات على العنوان التالي:

السيد الأمين العام

للمجلس الوطني للثقافة والفنون والآداب

ص. ب: 28613 - الصفاة

الرمز البريدي 13147

دولة الكويت

هاتف: 22431704 (965)

www.kuwaitculture.org.kw

التنضيد والإخراج والتنفيذ

وحدة الإنتاج في المجلس الوطني

ISBN 978 - 99906 - 0 - 627 - 0

العنوان الأصلي للكتاب

Dark Territory:

The Secret History of Cyber War



Fred Kaplan

Published by arrangement with the original publisher, Simon & Schuster, Inc.

طُبع من هذا الكتاب ثلاثة وأربعون ألف نسخة

رجب 1440 هـ ـ مارس 2019

المواد المنشورة في هذه السلسلة تعبر
عن رأي كاتبها ولا تعبر بالضرورة عن رأي المجلس

المحتوى

هل يُمكن حدوث مثل هذا الأمر في الواقع؟

في يوم السبت 4 يونيو من العام 1983، كان الرئيس رونالد ريغان Ronald Reagan يقضي يومه في «كامب ديفيد»، مُستَرخِيا، يُطالع بعض الأوراق، ثم بعد تناول طعام العشاء، وكما كان يفعل في كثير من الأحيان، جلس لمشاهدة أحد الأفلام. كان عرض تلك الليلة[1] هو فيلم «ألعاب الحرب» (المناورات الحربية) WarGames، بطولة ماثيو برودريك Matthew Broderick الذي كان يُجَسِّد فيه دور فتى مُراهق، بارع في أمور التكنولوجيا، يخترق من دون قصد الحاسوب الرئيسي في «قيادة دفاع الفضاء الجوي لأمريكا الشمالية» (نوراد) North American Aerospace Defense Command (NORAD)، وظنا منه أنه يلعب لعبة حاسوبية جديدة، أوشك على إشعال حرب عالمية ثالثة.

«هذا التسلسل للأحداث وسَمَ المرة الأولى التي يتطرق فيها رئيس أمريكي، أو توجيه من البيت الأبيض، إلى ما سيُصطلح على تسميته لاحقا وسائل الحرب السيبرانية»

في صباح يوم الأربعاء التالي[2]، عاد ريغان إلى البيت الأبيض، وعقد اجتماعا حضره وزراء الخارجية، والدفاع، والخزانة، إلى جانب فريقه لشؤون الأمن القومي، ورئيس الهيئة المشتركة لرؤساء الأركان، وستة عشر من أعضاء الكونغرس البارزين. كان الاجتماع لمناقشة نوع جديد من الصواريخ النووية وأرجحيّة محادثات الأسلحة مع الروس. لكن ريغان لم يستطع إبعاد ذاك الفيلم عن ذهنه، وفجأة في لحظة ما، نحّى أوراقه جانبا، وسأل ما إذا كان أي شخص آخر قد شاهد ذلك الفيلم. لم يكن أحد قد شاهد الفيلم، إذ إنه كان قد عُرض من فوره في دور السينما في يوم الجمعة الأخير. ثم انطلق ريغان في عرض ملخص تفصيلي عن حبكة الفيلم الروائية. أجال بعض البرلمانيين النّظر في الغرفة، بابتسامات مكبوتة، أو بحواجب مقوّسة تعبيرا عن دهشتهم. قبل ذلك بأقل من ثلاثة أشهر، كان ريغان قد ألقى خطاب «حرب النجوم»، داعيا العلماء إلى استحداث أسلحة ليزرية يمكنها - في حالة الحرب - أن تسقط الصواريخ النووية السوفييتية حينما تندفع نحو أمريكا، ولم تلقَ الفكرة أي قبول؛ إذ إنها بدت فكرة غريبة ومجنونة. الآن، ما الذي كان الرجل العجوز بصدده؟

بعد أن انتهى ريغان من عرضه لملخص الفيلم، توجه إلى الجنرال جون فيسي John Vessey، رئيس الهيئة المشتركة لرؤساء الأركان، الضابط الأعلى في جيش الولايات المتحدة، وسأله: «هل يمكن حدوث مثل هذا الأمر في الواقع؟» هل يمكن لأحد اقتحام حواسيبنا المهمة شديدة الحساسية؟

قال فيسي، الذي نشأ متمرسا على مثل هذه الاستفسارات، إنه سوف ينظر في الأمر.

بعد ذلك بأسبوع عاد الجنرال بإجابته إلى البيت الأبيض. اتضح أن فيلم ألعاب الحرب (المناورات الحربية) لم يكن قط مستبعدا وغير معقول. قال فيسي: «السيد الرئيس، المسألة أسوأ كثيرا مما تظن».

فجّر سؤال ريغان سلسلة من المذكرات، ومجموعات العمل، والدراسات، والاجتماعات، اشترك فيها الكثير من الدوائر والمؤسسات المعنية. بعد مضي خمسة عشر شهرا، أسفرت تلك الجهود عن صياغة التوجيه الرئاسي السري المتعلّق بالأمن القومي «إن إس دي دي - 145» (NSDD-145)، وكان بعنوان «السياسة القومية بشأن الاتصالات وأمن نظم

المعلومـــات المؤللـة» (National Policy on Telecommunications and Automated Information Systems Security)، ووقع عليه ريغان في 17 سبتمبر من العام 1984.

كانت تلك الوثيقة استشرافية (تنبئية)، إذ إن باكورة الحواسيب المحمولة كانت قد وصلت حديثا إلى الأسواق، ولم يظهر مزودو الإنترنت العموميون الأوائل إلا بعد بضعة أعوام. مع ذلك لاحظ كاتبو التوجيه الرئاسي السري المتعلّق بالأمن القومي «إن إس دي دي - 145» أن هذه الأجهزة الجديدة - التي كانت الدوائر الحكومية والصناعات التكنولوجية المتقدمة قد بدأت في شرائها على نحو متسارع - كانت «أشد ما تكون عرضة للاعتراض[3]، والوصول الإلكتروني غير المصرح به، وصور الاستغلال التقني ذات الصلة». كانت أجهزة الاستخبارات الأجنبية المعادية بالفعل تخترق تلك المرافق «على نحو مكثّف»، وكان لدى «الجماعات الإرهابية والعناصر الإجرامية» أيضا القدرة على فعل ذلك.

هذا التسلسل للأحداث - السؤال غير المألوف الذي وجهه ريغان إلى الجنرال فيسي، متبوعا بوثيقة سياسات رائدة مبتكرة - وَسَم المرّة الأولى التي يتطرّق فيها رئيس أمريكي، أو توجيه من البيت الأبيض، إلى ما سيُصطلح على تسميته لاحقا «وسائل الحرب السيبرانية».

حتى تلك اللحظة لم تدم الضجة طويلا، إذ إنه بموجب التوجيه الرئاسي «إن إس دي دي145-»، صارت وكالة الأمن القومي هي المسؤولة عن تأمين جميع المخدمات الحاسوبية وشبكات الحواسيب في الولايات المتحدة، وكان هذا بالنسبة إلى الكثيرين يعد تجاوزا للحدود. كانت وكالة الأمن القومي هي أكبر أجهزة الاستخبارات الأمريكية، وأكثرها سرية وتكتّما. (كان أعضاء الوكالة يتمازحون فيما بينهم بأن الأحرف الأولى لاسم وكالة الأمن القومي National Security Agency كانت تعني «لا يوجد مثل هذه الوكالة No Such Agency»). أُسست وكالة الأمن القومي في العام [4]1952 بهدف اعتراض الاتصالات الأجنبية، وكان محظورا عليها صراحة أن تتجسس على الأمريكيين. لم يكن المدافعون عن الحريات المدنية في الكونغرس ليسمحوا لمرسوم رئاسي بأن يطمس هذا التمييز ويجعله ضبابيا.

ثم اندثرت المسألة، على الأقل في نطاق المستويات السياسية العليا. وحينما عاودت الظهور بعد ذلك باثني عشر عاما، بعد وابل من الاقتحامات السيبرانية الفعلية التي حدثت في أثناء فترة رئاسة بيل كلينتون Bill Clinton، كان قد مر وقت كاف إلى حد أن كبار المسؤولين في ذلك اليوم صُدموا بما بدا مفاجئا من ضعف البلاد وقابليتها للتأثر بهذا التهديد الذي بدا جديدا تماما، ولم يتذكر هؤلاء المسؤولون التوجيه الرئاسي السري المتعلّق بالأمن القومي «إن إس دي دي - 145»، فضلا عن كونهم لم يسمعوا به أصلا.

حينما تغيرت إدارة البيت الأبيض ثانية (ومن ثم تغير الحزب السياسي) مع انتخاب جورج دبليو بوش George W. Bush، تراجعت المسألة مجدّدا، على الأقل في نظر العامة، لا سيّما بعد الهجمات الإرهابية في 11 سبتمبر من العام 2001، التي أسفرت عن مقتل ثلاثة آلاف أمريكي. قليلون هم من كانوا يهتمون بالحروب السيبرانية الظنّية (النظريّة) في حين كانت البلاد تخوض حربا حقيقية بالرصاص والقنابل.

لكن خلف الأبواب المغلقة، ومع انتشار الإنترنت إلى أقصى بقاع الكرة الأرضية، كانت إدارة بوش تنسج وتجدل تقنيات الحرب السيبرانية مع خطط الحرب التقليدية، وكذلك فعلت المؤسسات العسكرية لعدة دول أخرى، سواء كانت صديقة أو خلاف هذا. برزت الحرب السيبرانية على أنها تهديد وفرصة على نحو تبادلي، فهي أداة للتجسس، وسلاح للحرب، يستطيع الخصوم استخدامها لإلحاق الأذى بأمريكا، وكانت أمريكا تستطيع استخدامها لإلحاق الأذى بخصومها.

أثناء فترة رئاسة باراك أوباما Barack Obama، أطلق العنان لوسائل الحرب السيبرانية، وظهرت في موازنة الدفاع كأحد القطاعات القليلة التي زادت مخصصاتها في حين بقيت بعض القطاعات الأخرى جامدة من دون تغيير أو تراجعت. في العام 2009 استحدث روبرت غيتس Robert Gates - أول وزير دفاع في عهد أوباما، وهو كان باقيا في منصبه من زمن إدارة بوش - قيادة سيبرانية مخصّصة. خلال الأعوام الثلاثة الأولى للقيادة السيبرانية[5] زادت موازنتها السنوية إلى ثلاثة أضعاف، من 2.7 مليار دولار إلى 7 مليارات دولار (بالإضافة إلى 7 مليارات دولار أخرى للأنشطة السيبرانية في الفروع العسكرية إجمالا)، في حين تضاعفت صفوف

فرق الهجوم السيبراني من 900 فرد إلى 4000 فرد، مع توقع أن تصل إلى 14000 فرد في نهاية العقد.

كان مجال السيبرانية يتصاعد ويتضخم في جميع أرجاء العالم؛ وبحلول منتصف فترة رئاسة أوباما، كانت أكثر من عشرين دولة قد شكّلت وحدات متخصصة في وسائل الحرب السيبرانية ضمن جيوشها. كان كل يوم يجلب معه تقارير بشأن هجمات سيبرانية جديدة تشنها الصين، وروسيا، وإيران، وسورية، وكوريا الشمالية، وغيرها، ليس فقط ضد الشبكات الحاسوبية الخاصة بالبنتاغون أو بمقاولي (متعهدي) وزارة الدفاع، ولكن أيضا ضد الشبكات الحاسوبية التي لدى البنوك، وتجار التجزئة، والمصانع، وشبكات الطاقة الكهربائية، والمنشآت المائية، أي كل الأشياء المتصّلة بشبكة حاسوبية. وبحلول أوائل القرن الحادي والعشرين، شمل ذلك كل شيء تقريبا. وعلى الرغم من قلّة المعلن في هذا الخصوص، كانت الولايات المتحدة - وبضع قوى غربية أخرى - هي أيضا تشن هجمات سيبرانية على الشبكات الحاسوبية الخاصة بدول أخرى.

لم تكن تلك التسللات شيئا جديدا، فبقدر قِدَم العصور الرومانية، كانت الجيوش تعترض اتصالات العدو. في الحرب الأهلية الأمريكية[6]، استخدم جنرالات الاتحاديين والكونفدراليين (الانفصاليين) أجهزة التلغراف الجديدة لإرسال أوامر مزيّفة إلى العدو. أثناء الحرب العالمية الثانية[7]، كسر خبراء التشفير البريطانيون والأمريكيون رموز الشّفرة الألمانية واليابانية، وكان هذا عنصرا أساسيا في انتصار الحلفاء (ظل بعد ذلك سرا طوال أعوام كثيرة). في العقود القليلة الأولى من الحرب الباردة كان الجواسيس الأمريكيون والروس يعترضون على نحو دوري منتظم اتصالات بعضهم ببعض من إشارات راديوية (لاسلكية)، وبث للموجات الميكروية (الميكروويف)، واتصالات هاتفية. لم يقتصر الهدف على جمع معلومات استخباراتية بشأن نوايا وقدرات الطرف الآخر، بل إضافة إلى ذلك، للحصول على أفضلية في الحرب الجسيمة المخيفة المقبلة.

على الرغم من ذلك اتخذت وسائل حرب المعلومات بعدا جديدا تماما في العصر السيبراني. حتى الحقبة الجديدة كانت طواقم «استخبارات الإشارة» (سيجينت SIGINT) تحتشد للتّنصّت على خطوط الهاتف ومسح السماوات بحثا عن

إلكترونات شاردة متناثرة، لكن هذا كل ما كانوا يستطيعون فعله، الاستماع إلى المحادثات، واسترجاع الإشارات. في العصر السيبراني حالما كانوا يخترقون حاسوبا ما كان بإمكانهم التجوال خفية في الشبكة المرتبطة به بأسرها؛ ولا يكادون يدخلون إلى الشبكة، حتى يكون في استطاعتهم ليس فقط قراءة أو تنزيل وتحميل الكثير من المعلومات، بل كانوا يستطيعون أيضا تغيير محتواها - تشويشه، أو إفساده، أو محوه - وتضليل أو إرباك المسؤولين المعتمدين عليها.

حالما كانت الحواسيب تُستخدم للتحكم في تشغيل كل شيء في الحياة تقريبا، مثل: أنظمة توجيه القنابل الذكية، وأجهزة الطرد المركزي في مختبر تخصيب اليورانيوم، وصمامات التحكم في السدود، والمعاملات المالية للبنوك، وحتى الآليات الداخلية للسيارات، ومنظمات الحرارة، وأجهزة الإنذار ضد السرقة، وأجهزة تحميص الخبز الكهربائية (المحامص الكهربائية)؛ حينئذ كان اختراق شبكة الحاسوب يمنح الجاسوس أو المحارب السيبراني القدرة على السيطرة على أجهزة الطرد المركزي، والسدود، والمعاملات البنكية؛ لتبديل إعداداتها، أو إبطائها، أو زيادة سرعتها، أو عرقلتها، أو حتى تدميرها.

كان إحداث هذا الضرر يتم من بُعد، وربما كان المعتدي موجودا على الطرف الآخر من العالم. وخلافا للقنبلة الذرية أو القذيفة الباليستية (التسيارية) العابرة للقارات(*)، التي كانت منذ فترة طويلة قد أنهت التحصّن بالبعد المكاني، فإن السلاح السيبراني لم يكن يتطلب مشروعا صناعيا ضخما وواسع النطاق، أو مجمعا من العلماء النابغين، كان كل ما يلزم لبنائه هو ملء غرفة من الحواسيب، وفرقة صغيرة من أشخاص متمرسين على استخدامها.

كان هناك تحول آخر، ألا وهو «الشبـــكة العنكبوتيـــة العالمية (الويب) World Wide Web»، مثلما صار يطلق عليها، ولم تكن سوى شبكة حاسوبية

(*) القذائف الباليستية Ballistic missile، هي نظام أسلحة استراتيجي ذاتي الدفع، يتخذ مسارا مقوسا من موقع الإطلاق إلى هدف محدد سلفا، تبدأ القذيفة بمسار تسارع موجه بمحرك صاروخي يعطيها الدفع المناسب، يتبعه مسار حر يتأثر حصرا بالجاذبية الأرضية واحتكاك الهواء، إلى أن تصل حمولة القذيفة إلى هدفها. يمكن أن تكون الصواريخ الباليستية قصيرة، أو متوسطة، أو بعيدة المدى؛ ويمكن أن تحمل مواد تقليدية شديدة الانفجار، وكذلك ذخائر كيميائية أو بيولوجية أو نووية؛ كما يمكن إطلاقها من الطائرات، والسفن، والغواصات بالإضافة إلى المنصات الأرضية المتنقلة. [المترجم].

تمددت وانبسطت عبر العالم. كان الكثير من البرامج المصنفة على أنها سرية تُشغَّل على هذه الشبكة نفسها، وكان اختلافها عن البرامج الأخرى يتمثل في أن محتوياتها كانت مشفّرة. لكن هذا كان أيضا يعني أنه، مع ما يكفي من الوقت والجهد، كان يمكن فك تشفيرها أو النفاذ إليها. في الأيام الخوالي كان الجواسيس إذا رغبوا في التنصّت على أحد الهواتف، فإنهم كانوا يضعون جهازا على دائرة واحدة. أما في الحقبة السيبرانية فالبيانات تتدفق عبر الإنترنت في لمح البصر بسرعة خاطفة، وفي حزم رقمية، غالبا ما تتخللها حزم تحتوي على بيانات تخص أناسا آخرين. من ثم لم يعد من الممكن تحري الدقة في استخلاص رسائل الإرهابيين المتبادلة عبر البريد الإلكتروني، أو ثرثرتهم عبر الهاتف الجوال (الخلوي)؛ إذ صارت بيانات وأحاديث الجميع مطروحة للاصطياد، ومن المحتمل أن تكون موضوعة بالفعل تحت مراقبة عين ساهرة دائمة اليقظة.

لقد ازداد التوقع بأن حروب المستقبل حتما ستكون حروبا سيبرانية، على الأقل في جزء منها؛ كان الفضاء السيبراني قد وُسِم رسميا على أنه «ميدان» للحرب، مثل الجو، والبر، والبحر، والفضاء الخارجي. ونظرا إلى سلاسة وانسيابية الشبكة الحاسوبية العالمية، وبسبب حزم البيانات، وإنترنت الأشياء، فإن الحرب السيبرانية لن تشتمل على الجنود، والبحارة، والطيارين فقط؛ ولكنها، حتما ستتضمن البقية منّا. حينما يكون الفضاء السيبراني في كل مكان، فإن الحرب السيبرانية يمكن أن تتسرب وتنضح عبر كل المسام الرقمية.

طوال الانتقالات بين الرؤساء، كانت أفكار وسائل الحرب السيبرانية إما مبعدة، أو مهجورة، أو منسية، لكنها لم تختف قط. طوال الوقت، وحتى قبل أن يشاهد رونالد ريغان فيلم «ألعاب الحرب» (المناورات الحربية) WarGames، كانت الجيوب السرية للجهاز الإداري للأمن القومي تواصل بذل الجهد الجهيد لسد أوجه قصور برمجيات الحاسوب وإصلاح عيوبها؛ ومع ذلك، كانت تستغل المزيد منها.

استطاع الجنرال جاك فيسي أن يجيب بصورة سريعة عن سؤال ريغان، في غضون أسبوع من اجتماع يوم 8 يونيو من العام 1983، حينما سأل الرئيسُ عما إذا كان يستطيع أحد اختراق الحواسيب العسكرية، مثلما فعل الطفل في ذلك الفيلم، ذلك لأن فيسي أخذ السؤال وطرحه على رجل يدعى دونالد لثام

Donald Latham[8]. كان لثام مساعدا لوزير الدفاع لشؤون القيادة، والسيطرة، والاتصالات، والاستخبارات - اختصارا «إيه إس دي»(سي3 آي) (ASD(C3I – وبهذه الصفة، كان هو حلقة الوصل بين البنتاغون ووكالة الأمن القومي، التي كانت هي ذاتها جزءا سريا جدا من وزارة الدفاع. كانت وكالة الأمن القومي تنتشر داخل مجمّع فسيح من البنايات المغلقة بمصاريع في منشأة «فورت ميد» Fort Meade العسكرية بولاية ماريلاند Maryland، ومحاطة بحراس مسلحين وبوابات عالية؛ ومقارنة بوكالة الاستخبارات المركزية الأكثر شهرة التي كان مقرها في ضاحية لانجلي Langley بولاية فيرجينيا Virginia، كانت وكالة الأمن القومي أكبر كثيرا، وأفضل تمويلا، وأشد ازدحاما. كان لثام - مثل العديد من المسؤولين السابقين (والمستقبليين) في منصبه - قد عمل في وكالة الأمن القومي، وكان لايزال لديه صلات هناك، ويعرف خصوصيات وعموميات استخبارات الإشارات وكيفية اقتحام أنظمة الاتصالات داخل أمريكا وخارجها.

كان هناك أيضا مكاتب سرية جدا لاستخبارات الاتصالات تخص كل فرع من فروع القوات المسلحة، مثل: «وكالة الاستخبارات الجوية» Air Intelligence Agency (التي سميت فيما بعد باسم «مركز سلاح الجو لوسائل حرب المعلومات» Air Force Information Warfare Center) في قاعدة «كيلي» الجوية بمدينة سان أنطونيو San Antonio في ولاية تكساس Texas، و«السرب 609 لوسائل حرب المعلومات» 609the Information Warfare Squadron في قاعدة «شاو» الجوية Shaw Air Force Base بمدينة سومتر Sumter في ولاية كارولاينا الجنوبية South Carolina، ومختبرات علم التشفير المتناثرة في سلاح البحرية، و«قسم تكنولوجيات الدفاع الحرجة (الحاسمة)» Critical Defense Technologies Division التابع لوكالة الاستخبارات المركزية، و«قسم العمليات التكنولوجية الخاصة» Special Technological Operations Division التابع لـ «جيه - 39» J-39، وهو مكتب مغمور في هيئة الأركان المشتركة بالبنتاغون، لا يعرف بشأنه سوى عدد قليل (الدخول إليه يتطلب معرفة مجموعة من الأرقام السرية لتزويل الأقفال المركّبة على بابين معدنيين). كانت تلك الكيانات جميعا تتغذى من مراكز شعوذة ما وراء السري جدا نفسها وتغذيها؛ بعضها

تم تطويره داخليا، وبعضها صنّعته شركة «مختبر الأنظمة الكهرومغناطيسية» Electromagnetic Systems Laboratory (ESL,Inc)(*)، ومقاولون (متعهدون) متخصصون آخرون، وكان جميعها يتعامل مع وكالة الأمن القومي بطريقة أو بأخرى.

حينما سأل ريغان الجنرال فيسي عما إذا كان أحد يستطيع حقيقةً اختراق الحواسيب العسكرية، كان هذا بعيدا جدا عن المرّة الأولى التي كان السؤال قد طرح فيها. أما بالنسبة إلى أولئك الذين كانوا سيكتبون التوجيه الرئاسي السري المتعلّق بالأمن القومي «إن إس دي دي145-»، فكان السؤال بالفعل قديما جدا، مثل قِدَم الإنترنت ذاتها.

في أواخر الستينيات من القرن العشرين، قبل فترة طويلة من مشاهدة رونالد ريغان لفيلم «ألعاب الحرب (المناورات الحربية)»،اضطلعت وزارة الدفاع ببرنامج كان يُطلق عليه أربانت ARPANET. كان الراعي المباشر للبرنامج هو «وكالة مشروعات البحوث المتقدمة» (أربا) Advanced Research Projects Agency (ARPA)، الجهة المسؤولة عن تطوير واستحداث أسلحة مُستقبلية لجيش الولايات المتحدة. كانت فكرة «أربانت» هي إتاحة وسيلة لمُقاولي (مُتعاقدي) الوكالة - العلماء في المختبرات والجامعات في جميع أنحاء البلاد - لتشارك البيانات، والأوراق البحثية، والاكتشافات على شبكة حاسوبية واحدة. بدت الفكرة منطقية، إذ إن المزيد والمزيد من الباحثين كانوا يستخدمون الحواسيب. فوفق ما كانت الأمور تسير، كان ينبغي تجهيز مكتب مدير «وكالة مشروعات البحوث المتقدمة» (أربا) بعدد من الوحدات الطرفية للتحكم في تشغيل الحواسيب يُماثل عدد المقاولين (المتعهدين) العاملين من الخارج، وأن يكون كل منها موصولا بجهاز مُودِم (مضمان) modem على خط هاتف مُنفصل، ووحدة طرفية للتواصل مع جامعة كاليفورنيا (لوس أنجلوس) UCLA، وأخرى للتواصل مع «معهد أبحاث ستانفورد» Stanford Research

(*) شركة «مختبر الأنظمة الكهرومغناطيسية» Electromagnetic Systems Laboratory (ESL,Inc)، كانت إحدى شركات التكنولوجيا المتطورة في الولايات المتحدة، وكانت تعمل في تصميم البرمجيات، وتحليل النظم، وتطوير الأجهزة لسوق الاستطلاع الاستراتيجي. أُسست الشركة في يناير من العام 1964 في بالو ألتو Palo Alto بولاية كاليفورنيا California، وكانت رائدة في تطوير الأنظمة الاستراتيجية لمعالجة الإشارات، وأحد أبرز موردي أنظمة الاستطلاعات التكتيكية والتوجيهية إلى جيش الولايات المتحدة. [المترجم].

Institute، وثالثة للتواصل مع «جامعة يوتا» University of Utah، وما إلى ذلك. لذلك، فإن وجود شبكة واحدة تربط بينها جميعا، لن يقتصر على كونها أجدى من الوجهة الاقتصادية، بل إنها أيضا كانت ستُمَكِّن العلماء في كل أنحاء البلاد من تبادل البيانات من دون قيود، وعلى نحو أكثر حرية؛ إنها ستكون بمنزلة عطيّة للبحث العلمي.

في أبريل من العام 1967[9]، قبل بدء برنامج «أربانت» بفترة وجيزة، كتب مهندس يُدعى ويليس وير Willis Ware بحثا بعنوان «الأمن والخصوصية في أنظمة الحاسوب» Security and Privacy in Computer Systems، وقدمها في «المؤتمر نصف السنوي المُشتَرك للحاسوب» Joint Computer Conference الذي عُقِد في مدينة نيويورك. كان وير رائدا في مجال الحواسيب، ويعود تاريخه المهني إلى أواخر الأربعينيات من القرن العشرين، حينما كان مثل هذا المجال تخصصا نادرا. كان وير قد عمل في معهد «برينستون للدراسات المتقدمة» Princeton's Institute for Advanced Studies، وكان أحد تلاميذ جون فون نيومان John von Neumann[*]، حيث ساعد على تصميم أحد الحواسيب الكهربائية الأولى. وطوال أعوام، ترأس وير قسم علوم الحاسوب في مؤسسة «راند» RAND، وهي مجمَع فكر وبحث يُمَوله سلاح الجو، ومقرها مدينة سانتا مونيكا Santa Monica بولاية كاليفورنيا California. فهم وير جيدا وجهة النظر من أربانت[10]، وأشاد بأهداف البرنامج، وكان مُعجبا بطموحه، لكنه كان قلقا بشأن بعض آثاره التي كان مديروه قد تجاوزوا عنها.

طرح وير في بحثه الأخطار الناجمة عما سماه شبكات «تشارُك الموارد» resource-sharing الحاسوبية وشبكات الحواسيب «دائمة الاتصال» on-line، فمادامت الحواسيب موجودة في غرف معزولة، فلن يكون أمنها مشكلة. لكن، حالما تُتاح لعدة مُستخدمين إمكانية الوصول إلى البيانات من مواقع لا تتمتع بالحماية،

(*) جون فون نيومان John von Neumann[28] (ديسمبر 1903 – 8 فبراير 1957)، هو عالم رياضيات أمريكي من أصل مجري، وبصفة عامة كان يعتبر من أفضل علماء الرياضيات في عصره، وكان له العديد من الإسهامات في الرياضيات، والفيزياء، والاقتصاد، والحوسبة، والإحصاء. أنشأ فون نيومان بنية المعالجة باستخدام الحاسوب التي يُطلق عليها «بنية فون نيومان» von Neumann architecture، وهي في الأساس آلات (ماكينات) يمكن إعادة برمجتها، ويمكن تحميلها في ذاكرة الحاسوب جنبا إلى جنب مع البيانات، وتوفر له أداء متعدد الأغراض، وقوامها خمسة عناصر أساسية، هي: وحدة الإدخال، وحدة الإخراج، ووحدة التحكم، ووحدة الحساب والمنطق، ووحدة الذاكرة، وجميع الحواسيب المستخدمة حاليا تعمل وفق هذا التصميم. [المترجم].

فإن أي شخص يمتلك مهارات معيَّنة كان سيُمكنه اختراق الشبكة، وبعد النفاذ إلى أحد أجزاء الشبكة، سيكون باستطاعته أن يجوب أنحاءها كيفما شاء.

كان وير مهتما بهذه المشكلة على نحو خاص[11] لأنه كان يعلم أن مقاولي (متعهدي) وزارة الدفاع كانوا قد طلبوا من البنتاغون التصريح لهم بتخزين ملفات مصنّفة على أنها سرية وملفات غير سرية معا على حاسوب واحد. مُجَددا، على أحد الأصعدة، كانت الفكرة منطقية، إذ إن الحواسيب كانت باهظة التكلفة، وأن مَزْج كل البيانات معا كان من شأنه توفير كثير من المال. لكن، في زمن «أربانت» الوشيك، كان يمكن أن يثبُت أن هذه الممارسة كارثية، ففي حالة تسلل أي جاسوس مُخترقا الشبكات غير السرية، التي لم تكن محمية البتة، فإنه سيكون في إمكانه العثور على «أبواب خلفية» تؤدي إلى أقسام الشبكة المصنفة على أنها سرية. بعبارة أخرى، إن وجود شبكة حاسوبية، وحده، أوجد ثغرات أمنية حرجة (حساسة)، ولم يعد الاحتفاظ بالأسرار أمرا ممكنا.

حصل على ذلك البحث ستيفن لوكاسيك Stephen Lukasik، نائب مدير «وكالة مشروعات البحوث المتقدمة» (أربا) والمشرف على برنامج «أربانت»، وأخذه إلى لورانس روبرتس Lawrence Roberts، كبير علماء المشروع. قبل ذلك بعامين، كان روبرتس قد صمم وصلة اتصالات عبر خط هاتفي بسرعة 1200 بود(*)، تربط بين حاسوب في مُختبر «لينكولن» بمعهد ماساتشوستس للتكنولوجيا، حيث كان يعمل روبرتس في ذلك الوقت، وحاسوب أحد زملائه في مدينة سانتا مونيكا Santa Monica. كانت تلك هي المرة الأولى التي يتحقق فيها هذا الإنجاز الفذ. في الواقع، كان روبرتس هو ألكسندر جراهام بيل Alexander Graham Bell عصر الحاسوب؛ ومع ذلك، لم يكن روبرتس قد فكر في أمن وحماية تلك الوصلة. حقيقة، أزعجه البحث الذي أعده وير، وتوسل إلى لوكاسيك ألا يُثقِل على فريقه ويُحمّله عبء مُتَطَلَب أمني، كان الأمر سيبدو أشبه بإخبار الأخوين رايت بأن طائرتهما

(*) بود Baud، هو وحدة لقياس معدل الترميز، أحد المكونات التي تُحدد سرعة الاتصال عبر قناة بيانات، ويعبر البود عن عدد مرات تغير حالة الإشارة الإلكترونية في الثانية الواحدة. اشتُق اسم وحدة البود من اسم المهندس الفرنسي جان موريس إميل بودو Jean-Maurice-Emile Baudot، مخترع نظام «ترميز بود» في التلغراف، واستُخدمت وحدة البود لأول مرة لقياس سرعة إرسال التلغراف. يرتبط معدل البود بـمعدل سرعة المعلومات الذي يُقاس بالبت في الثانية bit per second (bps)، لكن ينبغي عدم الخلط بينهما. [المترجم].

الأولى في كيتي هوك Kitty Hawk(*) ينبغي أن تطير مسافة خمسين ميلا حاملة على متنها عشرين مسافرا. قال روبرتس: دعنا نقم بهذا خطوة فخطوة. كان جَعْل النظام يعمل أمرا صعبا بما فيه الكفاية، ولم يكن في استطاعة الروس بناء شيء مثل هذا على مدى عدة عقود.

كان روبرتس مُحقا. كان الأمر سوف يستغرق من الروس (والصينيين وغيرهم) عقودا - نحو ثلاثة عقود – من أجل بلورة وبناء نسختهم من «أربانت» والتكنولوجيا التي تُمكنهم من التسلل إلى «أربانت» الأمريكية. في غضون ذلك، كانت نظم وشبكات واسعة تنمو وتنتشر في جميع أنحاء الولايات المتحدة وفي معظم العالم، من دون أي أحكام وتدابير تخص تأمينها.

على مدار الأربعين عاما اللاحقة، عمل وير استشاريا في المجالس واللجان الحكومية المعنية بأمن الحاسوب وخصوصيته. في العام 1980، كان لورانس لاسكر Lawrence Lasker ووالتر باركِز Walter Parkes[12]، اللذان تزاملا في السابق في جامعة «يال» Yale حينما كانا في أواخر العشرينيات من العمر، يكتبان سيناريو الفيلم الذي كان سيُطلق عليه اسم «ألعاب الحرب» (المناورات الحربية). ساورهما ارتياب بشأن معقولية جزء من الخط الرئيسي للحبكة الروائية لقصة الفيلم، وكان أحد أصدقائهما من قراصنة الحاسوب «الهاكرز» hacker قد أخبرهما بشأن برمجية «عِفْريت الاتصال الهاتفي» demon-dialing (يُطلق عليها أيضا «حرب النداء الهاتفي»)، التي بها يبحث «مُودِم» modem الهاتف عن أجهزة مُودِم أخرى في الجوار، بأن يهاتف المُودِم تلقائيا كل رقم هاتف يحمل الرمز المحلي للمنطقة، ويدعه يُحدث رنينا لمرتين قبل الانتقال إلى مُهاتفة الرقم التالي. إذا أجاب أحد أجهزة المُودِم، فإنه كان سيُصدر نعيقا (صراخا)، في هذه الحالة كانت برمجية «عِفْريت الاتصال الهاتفي» ستسجل ذلك الرقم، وسيُعاود مُختَرِق الحاسوب (الهاكرز) الاتصال به لاحقا. (هذا هو الأسلوب الذي كان مهووسو

(*) كيتي هوك Kitty Hawk هي مدينة في مقاطعة دير Dare بولاية كارولينا الشمالية North Carolina، أُسست في أوائل القرن الثامن عشر باسم «تشيكاهوك» Chickahawk. اكتسبت «كيتي هوك» شهرة على مستوى العالم بعد أن قام الأخوان رايت، في 17 ديسمبر 1903، بأول رحلة طيران تعمل بالطاقة في مدينة كيل ديفيل هيلز Kill Devil Hills، التي تبعد ستة كيلومترات جنوب المدينة. وبعد الرحلة، سافر الأخوان إلى «كيتي هوك» حيث أرسلا برقية إلى والدهما لإبلاغه بنجاح تجربتهما. [المترجم].

الحاسوب الأوائل يتبعونه لعثور بعضهم على بعض، وهو أحد أشكال عصر ما قبل الإنترنت لما يُعرف باسم «تصيُّد الويب» (web trolling). في النص السينمائي (السيناريو)، كانت هذه هي الكيفية التي يستخدمها بطلهما الفتى النابغة ليتسلل إلى حاسوب «قيادة دفاع الفضاء الجوي لأمريكا الشمالية» (نوراد) ، لكن لاسكر وباركز تساءلا عما إذا كان هذا ممكنا، ألن يكون حاسوب عسكري معزولا عن خطوط الهاتف العمومية؟

كان «لاسكر» يعيش في مدينة سانتا مونيكا، على بُعد بضع بنايات من مؤسسة «راند» RAND. فكر في أنه ربما يكون هناك شخص ما ذو فائدة، اتصل لاسكر هاتفيا بمسؤول الشؤون العامة في مؤسسة «راند» RAND، فأوصله بـ وير، الذي دعاه هو وباركز إلى الحضور إلى مكتبه.

لقد وجدا الرجل المناسب. كان وير قد عرف منذ فترة طويلة بشأن أوجه الضعف والثغرات الأمنية التي لا حصر لها الموجودة في شبكات الحاسوب، إضافة إلى ذلك، كان قد ساعد على تصميم البرمجيات في «قيادة دفاع الفضاء الجوي لأمريكا الشمالية» (نوراد). بالنسبة إلى شخص منهمك وغارق تماما في عالم الأسرار الكبرى، كان وير على نحو ملحوظ مُنفتحا، بل إنه حتى كان ودودا. كان يبدو مثل شخصية جيمني كريكيت Jiminy Cricket في فيلم ديزني الكرتوني «بينوكيو» Pinocchio(*)، وكان أيضا يتصرف مثله بعض الشيء: متحمس، وسريع البديهة، ويسارع إلى الضحك.

عندما استمع وير لأسئلة الثنائي لاسكر وباركز، بدد مخاوفهما، بعد ذلك أجابهما: «نعم»، وأخبرهما بأنه مُفترَض أن يكون الحاسوب في «قيادة دفاع الفضاء الجوي

(*) بينوكيو Pinocchio شخصية خيالية وبطل رواية الأطفال «مُغامرات بينوكيو» Adventures of Pinocchio (1883) للكاتب الإيطالي «كارلو كولودي» Carlo Collodi. نُحت «بينوكيو» على يد نحات خشب يُدعى جيبيتو Geppetto في قرية بالقرب من مدينة لوكا Lucca الإيطالية. صُنع «بينوكيو» كدُمية خشبية لكنه حلم بأن يصبح فتى حقيقيا، واتسم بميله المتكرر إلى الكذب، مما يجعل أنفه يطول. قُدمت قصته في قوالب فنية أخرى، لاسيما فيلم «بينوكيو» من إنتاج ديزني في العام 1940 الذي قُدمت فيه شخصية «جيمني كريكيت» Jiminy Cricket على نحو يختلف عن نسخته الإيطالية الأصلية «كريكيت المتحدث» Talking Cricket، وهو شخصية خيالية ابتكرها الكاتب الإيطالي كولودي في روايته كشخصية غير معروفة، حُوّل في نسخة ديزني إلى شريك هزلي وحكيم يرافق «بينوكيو» في مغامراته، بعد أن عُين من قِبَل الجنية الزرقاء (المعروفة في الكتاب باسم الجنية ذات الشعر الفيروزي) ليكون بمنزلة الضمير الرسمي لبينوكيو. يختلف تصميمه عن صراصير الليل الحقيقية، فهو يرتدي مثل رجل نبيل من القرن التاسع عشر. منذ بدايته في «بينوكيو»، أصبح شخصية ديزني الأيقونية، وظهر في العديد من الأعمال الأخرى. [المترجم].

لأمريكا الشمالية» (نوراد) معزولا، لكن بعض الضباط رغبوا في العمل من منازلهم في أثناء عطلة نهاية الأسبوع، لذا فقد تركوا منفذا مفتوحا. كان أي شخص يستطيع الولوج إذا اتصل هاتفيا بالرقم الصحيح. كان وير يُطلِع كُتَّاب النص السينمائي (السيناريو) حديثي العهد على سر لا يعرفه سوى القليل من زملائه. ابتسم وير ابتسامة خبيثة وهو يخبرهما بأن الحاسوب الوحيد الآمن تماما، هو الحاسوب الذي لا يستطيع أحد استخدامه.

منح وير الثنائي لاسكر وباركِز الثقة للمُضي قدما في مشروعهما. لم يكن أي منهما يرغب في كتابة خيال محض، وأرادا إضفاء مِثقال ذرة من المِصداقية حتى إلى حبكات الفيلم الدرامية المُستبعدة، وقد منحهما وير ذلك. إن جانبا كبيرا من سيناريو فيلم «ألعاب الحرب» (المناورات الحربية)، الذي أثار فضول رونالد ريغان وأدى إلى أول نهج قومي للحد من الثغرات الأمنية في الحواسيب، كان من الملائم أن يكون من إبداع الرجل الذي كان أول من حذّر من أن الحواسيب غير حصينة ومعرضة للخطر.

لم يكن وير يستطيع أن يُصرِّح بذلك، لكن إلى جانب عمله لمصلحة مؤسسة «راند» RAND، خدم أيضا في «المجلس الاستشاري العلمي» Scientific Advisory Board التابع لـ «وكالة الأمن القومي» National Security Agency. كان وير يعرف الوسائل الكثيرة التي كانت تستخدمها فرق استخبارات الإشارات التابعة لوكالة الأمن القومي، لتخترق بها الدروع للنفاذ إلى الاتصالات الراديوية (اللاسلكية) والهاتفية للمؤسسات العسكرية الروسية والصينية. في ذلك الوقت، لم يكن لدى أي من تلك الدول حواسيب، لكن شبكة «أربانت» كانت مُتصلة عبر خطوط الهاتف من خلال أجهزة مُودِم. عرف وير أن روسيا أو الصين كان يمكنهما اختراق خطوط الهاتف الأمريكية، ومن ثم اختراق شبكة «أربانت»، مستخدمين الحيل ذاتها التي كانت أمريكا تستخدمها لاختراق خطوط الهاتف لديهما.

بعبارة أخرى، ما كانت تفعله الولايات المتحدة بأعدائها، كان في إمكان أعدائها فعله بالولايات المتحدة، ربما ليس في الوقت الحالي، ولكن في يوم ما قريب.

كانت جذور وكالة الأمن القومي[13] تعود إلى الحرب العالمية الأولى. في أغسطس من العام 1917، بعد فترة وجيزة من انضمام الولايات المتحدة إلى المعركة، أنشأت

حكومة الولايات المتحدة «فرع الاستخبارات العسكرية 8» (إم آي - 8) Military Intelligence Branch 8 (MI-8) ، الذي كان مُخَصصا لفك رموز شفرة إشارات البرق (التلغراف) الألمانية. ظلت الوحدة قائمة إلى ما بعد الحرب، تحت رعاية مزدوجة من وزارتي الحربية والخارجية، داخل بناية لا تجذب الانتباه في مدينة نيويورك، وكان المنتمون إلى الوحدة يطلقون عليها اسم «الغرفة السوداء» the Black Chamber. كان الاسم الرمزي (الحركي) للوحدة هو «رَهْط تحويل الكود» Code Compilation Company، وكانت ترصد اتصالات عناصر كان يُشتبه في أنهم مخربون؛ كانت كبرى ضرباتها المفاجئة هي إقناع شركة ويسترن يونيون Western Union بإتاحة إمكانية الوصول إلى جميع البرقيات المنقولة عبر أسلاكها. في النهاية، أُغلقت «الغرفة السوداء» في العام 1929، بعد أن أعلن وزير الخارجية هنري ستيمسون Henry Stimson: «أيها السادة المحترمون، لا تطلعوا على رسائل البريد الإلكتروني لبعضكم البعض». لكن، مع اندلاع الحرب العالمية الثانية، جرى إحياء هذه الممارسة على أنها «وكالة أمن الإشارة» Signal Security Agency، التي كانت - جنبا إلى جنب مع نظراء بريطانيين - تكسر رموز شفرة الاتصالات الألمانية واليابانية، وهو العمل الذي ساعد الحلفاء على حسم الحرب لمصلحتهم. بعد ذلك، تحولت إلى «وكالة أمن الجيش الميداني» (القوات البرية) Army Security Agency، ثم «وكالة أمن القوات المسلحة» Armed Forces Security Agency مُتعددة الفروع. ثم في العام 1952، حينما أدرك الرئيس هاري ترومان Harry Truman أن الفروع لم يكن بعضها يتعاون مع بعض، صارت مؤسسة موحدة لكسر الشفرة أُطلق عليها اسم «وكالة الأمن القومي» National Security Agency.

طوال فترة الحرب الباردة، كانت وكالة الأمن القومي تُقيم قواعد حول العالم؛ هوائيات ضخمة، وأطباقا لاقطة (أطباق هوائي الرادار)، ومحطات استماع في المملكة المتحدة، وكندا، واليابان، وألمانيا، وأستراليا، ونيوزيلندا؛ بهدف اعتراض، وترجمة، وتحليل كل أساليب الاتصالات داخل الاتحاد السوفييتي. كذلك، وبالاشتراك مع سلاح الجو، أرسلت وكالة الاستخبارات المركزية (سي آي إيه CIA) طائرات للاستخبارات الإلكترونية تُحَلِّق على طول الحدود السوفييتية لالتقاط الإشارات، وفي بعض الأحيان

عبر الحدود؛ وفي عمليات انطوت على أخطار أكبر، أرسل سلاح البحرية غواصات مجهزة بالهوائيات والكابلات، إلى الموانئ (المرافئ) السوفييتية.

في الأعوام الأولى من الحرب الباردة، كان الجميع يستمعون أساسا للإشارات الراديوية (اللاسلكية)، التي كانت ترتد من الأيونوسفير في كل أرجاء الكرة الأرضية. كان أي هوائي قوي، أو طبق لاقط كبير، يُمكنه التقاط الإشارات من أي مكان تقريبا. بعد ذلك، في السبعينيات من القرن العشرين، بدأ الروس في التحول إلى أجهزة الإرسال بالموجات الميكروية (ميكروويف)، التي كانت تُبَث عبر مسافات أقصر بكثير، وكان ينبغي وضع أجهزة الاستقبال على خط رؤية مباشر مستقيم مع الشعاع حتى يُمكن اعتراضه. لذا، أنشأت وكالة الأمن القومي برامج مُشتركة، وأرسلت جواسيس من وكالة الاستخبارات المركزية أو من دوائر أخرى خلف خطوط العدو، بالأساس في دول حلف وارسو في أوروبا الشرقية، لإقامة مراكز استماع تبدو مثل علامات الطرق السريعة، أو أعمدة الهاتف، أو غيرها من الأشياء المعتادة.

ركَّبت وكالة الأمن القومي مجموعة هائلة من معدات الاستخبارات الإلكترونية في الطابق العاشر من السفارة الأمريكية، داخل العاصمة موسكو، المدينة التي بها عدد قليل من ناطحات السحاب، لذا كان الطابق العاشر يُتيح إطلالة بانورامية. جمعت أجهزة استقبال الموجات الميكروية (ميكروويف) مُحادثات هاتفية بين كبار المسؤولين السوفييت - بمن في ذلك الرئيس ليونيد بريجنيف Leonid Brezhnev ذاته – وهم يجوبون أرجاء المدينة مُستقلين سياراتهم الليموزين.

اشتبهت وكالة الاستخبارات السوفييتية (كي جي بي KGB) في أن شيئا غريبا يحدث هناك في الأعلى. في 20 يناير من العام 1978، استيقظ بوبي راي إنمان Bobby Ray Inman، مدير وكالة الأمن القومي، على اتصال هاتفي من وارين كريستوفر Warren Christopher، نائب وزير الخارجية. كان حريق قد اندلع في السفارة الأمريكية بموسكو، وكان رئيس قسم الإطفاء الداخلي يقول إنه لن يستطع إخماده إلا إذا سُمح له بالدخول إلى الطابق العاشر. استفسر كريستوفر من إنمان عما ينبغي له فعله.

أجاب إنمان: «دعه يحترق». (على أي حال، في النهاية أخمد رجال الإطفاء الحريق. كان واحدا من حرائق عدة اندلعت بشكل غامض في السفارة خلال تلك الحقبة).

بحلول العام 1980، آخر عام كامل من فترة رئاسة جيمي كارتر Jimmy Carter، كانت دوائر التجسس الأمريكية قد نفذت إلى الآلة العسكرية السوفييتية، وتوغلت فيها بعمق من نواحٍ عديدة، حتى إن المحللين كانوا يستطيعون تجميع صورة شبه كاملة لعملياتها، وأنماطها، ونقاط قوتها وضعفها؛ وأدركوا أن الجيش السوفييتي كان غير حصين وعرضة للهجوم، على الرغم من تعزيزاته الهائلة في القوات والدبابات والصواريخ.

كانت الثغرات الفتاكة تكمن في روابط الاتصالات في أنظمة القيادة والسيطرة، وهي الوسيلة التي كان مشغلو الرادارات يتتبعون بها الطائرات والصواريخ الآتية. ومن خلالها أيضا كان كبار ضباط هيئة الأركان يرسلون الأوامر، وكان كبار المسؤولين في الكرملين يقررون ما إذا كانوا سيخوضون الحرب. وحالما تكون طواقم «استخبارات الإشارة» (سيجينت) الأمريكية قد دلفت إلى داخل أنظمة القيادة والسيطرة السوفييتية، لم يكن باستطاعتهم فقط معرفة ما الذي كان يخطط له الروس، وهو في حد ذاته أمر ثمين وذو قيمة بما فيه الكفاية، بل كان يمكنهم أيضا إدراج معلومات خاطئة، أو عرقلة إشارات أوامر القيادة، أو حتى إيقاف تشغيل نظام القيادة والسيطرة. تلك الاضطرابات في حد ذاتها، ربما لم تكن تؤدي إلى حسم الحرب، لكن كان بإمكانها أن تخل بالتوازن، وتشيع الارتباك في صفوف الضباط السوفييت، وتجعلهم يرتابون فيما يرونه من معلومات استخباراتية، وفي الأوامر التي يتلقونها؛ الأمر الذي - في أفضل السيناريوهات - ربما يمنعهم من شن حرب في الأساس.

بحلول ذلك الوقت كان الروس قد عرفوا تشفير قنوات القيادة والسيطرة الأكثر أهمية، لكن وكالة الأمن القومي كانت تدرك كيفية كسر رموز الشفرة، أو على الأقل بعض منها. حينما كان خبراء الشفرة من أي جنسية يشفرون إشارة ما، فهم عادة ما كانوا يرتكبون أخطاء هنا وهناك، تاركين بعض المقاطع في هيئة نص عادي. كانت عملية فك شفرة إحدى الرسائل تعتمد على العثور على الخطأ، والعمل بشكل عكسي لمعرفة الكيفية التي شُفِّرَ بها مقطع ما في بلاغات سابقة، على سبيل المثال: تحية ترحيب تستخدم كثيرا أو مصطلحات عسكرية معتادة، ومن ثم تُكشف رموز التشفير.

كان بوبي راي إنمان مديرا للاستخبارات البحرية قبل أن يتولى إدارة وكالة الأمن القومي في العام 1977، في بداية عهد الرئيس كارتر. حتى حينها كان إنمان ومعاونوه يعبثون بألغاز التشفير. وبعد أن أصبحت تحت تصرفه الموازنة السرية الهائلة لوكالة الأمن القومي، انطلق إنمان في أداء المهمة بكامل قوته. كان الأمر يتطلب معدات قادرة على تخزين الكثير من البيانات ومعالجتها بسرعة عالية لمقارنة المقاطع المشفرة بالأخطاء على نحو سليم. طوال أعوام كثيرة، صممت وكالة الأمن القومي حواسيب كانت تملأ ممرات واسعة، لكن هذه المهمة الجديدة كانت تفوق مقدرة الوكالة. لذا، في أوائل فترة رئاسته للوكالة، بدأ إنمان برنامجا أطلق عليه «ترقية كفاءة الإشارات المُرَمَّزة» (بي إس يو) (Bauded Signals Upgrade (BSU، وكان البرنامج يتضمن أول «حاسوب فائق» (supercomputer). كان الحاسوب الواحد يكلف أكثر من مليار دولار أمريكي، وكانت منفعته قصيرة الأجل، إذ إنه بمجرد أن يدرك السوفييت أن رموز شفرتهم قد كُسرت، فإنهم يبتكرون رموزا جديدة، ومن ثم كان سيتعين على خبراء فك الشفرة في وكالة الأمن القومي البدء من جديد. لكن في فترة وجيزة من غفلة الروس، ساعد برنامج «ترقية كفاءة الإشارات المرمزة» (بي إس يو) على كسر ما يكفي من الرموز عالية المستوى؛ وإلى جانب المعرفة المكتسبة من الاختراقات الأخرى، أدى ذلك إلى اكتساب الولايات المتحدة أفضلية - ربما كانت حاسمة - في العنصر الأشد فتكا في تنافس الحرب الباردة.

كان لإنمان حليف قوي ضمن كبار علماء البنتاغون هو ويليام بيري William Perry، الذي كان طوال ربع قرن من الزمان قد انهمك في تلك الطريقة من التفكير على وجه التحديد. بعد انتهائه من الخدمة العسكرية في الجيش الميداني (القوات البرية) عند نهاية الحرب العالمية الثانية، نال بيري درجات علمية متقدمة في الرياضيات، وحصل على وظيفة في «مختبرات سيلفانيا» (Sylvania Labs)، وهي واحد من الكثير من مقاولي (متعهدي) الدفاع في مجال التكنولوجيا المتقدمة التي كانت تبزغ في ولاية كاليفورنيا الشمالية، وهي المنطقة التي أُطلق عليها لاحقا اسم «وادي السيليكون» (Silicon Valley). بينما كان العديد من تلك الشركات تعمل على تصميم أنظمة الرادار والأسلحة، كانت «مختبرات سيلفانيا» متخصصة في التدابير الإلكترونية المضادة، وهي أجهزة تشوش على الأنظمة الإلكترونية، أو

تعمل على تحييدها أو تعطيلها. كان أحد المشروعات الأولى التي عمل بها بيري معنيا باعتراض الإشارات الراديوية (اللاسلكية) التي توجه رأسا حربيا نوويا سوفييتيا في أثناء هبوطه نحو هدفه، ثم تغير مساره لينحرف الرأس الحربي عن وجهته. كان بيري قد اكتشف أسلوبا لفعل ذلك، لكنه أخبر رؤساءه بأن هذا لن يكون ذا فائدة كبيرة، لأن الرؤوس الحربية النووية السوفييتية كانت قوية جدا، وتحدث انفجارا بقوة عدة آلاف من الأطنان، فضلا عن اللهيب الحراري والسقاطة المشعة (الغبار المشع)، حتى إن ملايين الأمريكيين كانوا سيلقون حتفهم بكل الأحوال. (بعد مضي عدة أعوام، أدت هذه الخبرة إلى أن يصير بيري مؤيدا بارزا لمعاهدات الحد من الأسلحة النووية).

مع ذلك فَطِن بيري إلى نقطة جوهرية لم يتبينها في ذلك الحين معظم علماء الأسلحة الآخرين، وهي أن الوصول إلى داخل اتصالات العدو كان يمكن أن يغير من تأثير السلاح على نحو جذري، وربما يغير نتيجة معركة أو حرب.

ارتقى بيري في المراتب في مختبرات سيلفانيا إلى أن تولى منصب المدير في العام 1954. وبعد ذلك بعشرة أعوام غادرها ليؤسس شركته الخاصة باسم «مختبر الأنظمة الكهرومغناطيسية» (إي إس إل Electromagnetic Systems Laboratory (ESL)، التي قامت بأعمال تعاقدية حصريا تقريبا لمصلحة وكالة الأمن القومي ووكالة الاستخبارات المركزية. حينما التحق بيري بالبنتاغون في العام 1977 كان ملما بما لدى دوائر التجسس من أوجه تطور في مجال استخبارات الإشارات، شأنه في ذلك شأن أي شخص آخر من بقية أعضاء البنتاغون. في نهاية المطاف، كانت شركته قد بنت المعدات والتجهيزات التي جعلت معظم ذلك التقدم ممكنا.

كان بيري هو الذي وضع تلك التطورات المبعثرة تحت مبدأ موحد، هو: «وسائل الحرب المضادة للقيادة والسيطرة» (counter-C2 warfare). استمد بيري هذه العبارة من انشغاله فترة طويلة بالتدابير الإلكترونية المضادة، على سبيل المثال التشويش على جهاز استقبال الرادار بطائرات العدو. لكن بينما كانت أجهزة التشويش تمنح الطائرات أفضلية تكتيكية، كانت وسائل الحرب المضادة للقيادة والسيطرة هي مفهوما استراتيجيا. كان هدفها هو الحط من قدرة قيادة العدو على خوض الحرب. كان المفهوم يتعلق بوصلات الاتصالات وتكنولوجيا اعتراضها، أو

عرقلتها، أو فصلها، ليس فقط بوصفها السير المتحرك الناقل للأعمال الحربية، لكن بوصفها سلاحا حاسما في حد ذاتها.

حينما أحيط جيمي كارتر علما بتلك الطفرات الاستراتيجية، بدا أنه مفتون بالتكنولوجيا. لكن، خليفته رونالد ريغان Ronald Reagan، وهو من صقور الحرب الباردة، حينما سمع المعلومات ذاتها بعد مرور عام، أظهر قدرا ضئيلا من الاهتمام بالتفاصيل التقنية، لكن جل اهتمامه كان منصبا على الصورة العامة الأشمل. كان هذا يعني أنه إذا اندلعت الحرب بين القوى العظمى، وفق ما كان يرجح الكثيرون، كانت الولايات المتحدة تستطيع أن تكسب الحرب، وربما على نحو سريع وحاسم. في فترته الرئاسية الثانية[14]، أعاد ريغان التفكير في تداعيات التفوق الأمريكي، لا سيما بعد أن تولى الإصلاحي ميخائيل جورباتشوف Mikhail Gorbachev الكرملين. أدرك ريغان أن أساليب جيشه العدائية وخطبه الصفيقة كانت تفزع الروس وتجعلهم شديدي الهياج، وتجعل العالم أكثر خطورة؛ لذا، خفف ريغان من حدة لهجته، وتواصل مع جورباتشوف، وانتهى بهما الأمر إلى توقيع سلسلة من الاتفاقيات التاريخية بشأن الحد من التسلح، التي «تقريبا» أعادت الاتحاد السوفييتي - «إمبراطورية الشر»، كما كان ريغان قد وصفه ذات مرة - إلى النظام الدولي. لكن في أثناء فترة رئاسته الأولى كان ريغان يجاهد ويضغط بقوة من أجل منفعته، إذ شجع وكالة الأمن القومي والدوائر الأخرى على مواصلة حملة التصدي للقيادة والسيطرة.

في خضم هذا الضغط لم يقف الروس مكتوفي الأيدي. حينما اكتشفوا أمر الموجات الميكروية (ميكروويف)[15] التي تنبعث من الطابق العاشر من سفارة الولايات المتحدة في موسكو، بدأوا في توجيه مولداتهم لبث موجاتهم الميكروية (ميكروويف) نحو نوافذ السفارة الأمريكية، آملين الاستماع إلى محادثات الجواسيس الأمريكيين.

نشأ الروس ماهرين في لعبة التجسس ومكافحته. في إحدى المراحل علم المسؤولون أن جهاز الاستخبارات الروسي (كي جي بي) كان بطريقة ما يسرق أسرارا من السفارة الأمريكية في موسكو. أرسلت وكالة الأمن القومي محللا يدعى تشارلز غاندي Charles Gandy ليعمل على حل اللغز. كان غاندي موهوبا، وماهرا في العثور على الأبواب السرية (الفخاخ)، والثغرات الأمنية في أي جهاز. سرعان ما عثر غاندي على

أداة يطلق عليها «جن مان» (القاتل المحترف) Gunman موضوعة داخل ست عشرة آلة كاتبة من طراز «آي بي إم سيليكتريك» (IBM Selectric) التي كان يستخدمها أمناء (سكرتارية) مسؤولي السفارة رفيعي المستوى. كانت الأداة «جن مان» (القاتل المحترف) تسجل كل ضربة (نقرة) لمفاتيح الآلة الكاتبة، وتنقل البيانات إلى جهاز استقبال موضوع في كنيسة عبر الشارع. (كشفت تحقيقات لاحقة أن جاسوسة روسية جذابة كانت قد استدرجت حارسا من السفارة للسماح لها بالدخول).

سرعان ما صار جليا أن الروس كانوا يجهزون أشعة موجات ميكروية (ميكروويف) وينشئون محطات استماع في كل أنحاء واشنطن العاصمة، ومدينة نيويورك. كان كبار المسؤولين في البنتاغون، أولئك الذين كانت نوافذ مكاتبهم مواجهة للبنايات العالية الموجودة عبر نهر بوتوماك Potomac River، يداومون على تشغيل موسيقى خفيفة من نوعية موزاك Muzak(*) في مكاتبهم أثناء العمل[16]، ومن ثم إذا كان هناك جاسوس روسي يطلق موجات ميكروية (ميكروويف) على تلك النوافذ، فإن الصوت المحيط كان سيشوشه، ويحجب محادثاتهم.

كان معاونو «بوبي راي إنمان» قد قيَّموا الضرر من هذا النوع الجديد من التجسس. كان الرئيس كارتر، المهندس المحنك تقنيا (الذي كان يحب فحص مخططات التصميمات الأولية لأحدث أقمار التجسس العسكرية الاصطناعية)، قد تلقى تأكيدات بأن اتصالاته الهاتفية، وكذلك اتصالات وزيري الخارجية والدفاع، كانت تنقل عبر خطوط أرضية مؤمنة. لكن، حينما تتبع تقنيو وكالة الأمن القومي تلك الخطوط، اكتشفوا أن الإشارة حالما تصل إلى ولاية ماريلاند Maryland كانت تُحوَّل إلى أجهزة إرسال تعمل بالموجات الميكروية (ميكروويف)، التي كانت عرضة للاعتراض. لم يكن هناك أي دليل على أن السوفييت كانوا يتنصتون، ولكن لم يكن هناك أي سبب لاعتقاد أنهم لم يكونوا يفعلون ذلك. بالتأكيد كان باستطاعتهم فعل ذلك، مع بعض الصعوبة.

(*) «موزاك» Muzak: هي علامة تجارية مسجلة منذ 21 ديسمبر 1954 للموسيقى الخفيفة التي تُشغَّل في الخلفية في متاجر التجزئة وغيرها من المؤسسات العامة، وغالبا ما يستخدم مصطلح «موزاك» - على الأقل في الولايات المتحدة - لمعظم أشكال موسيقى الخلفية، بغض النظر عن منشأ الموسيقى، وقد يعرف أيضا باسم «موسيقى المصعد». وعلى الرغم من أن شركة «موزاك» كانت سنوات عديدة هي أشهر مورد للموسيقى في الخلفية، فإنها ترتبط عادة بموسيقى المصاعد، غير أن الشركة لم توفر بنفسها الموسيقى للمصاعد. [المترجم]

استغرق الأمر بعض الوقت، ولكن كلما كان يُكتَشف المزيد من تلك الثغرات الأمنية، وكلما كان يظهر المزيد من الأدلة على أن جواسيس الاتحاد السوفييتي يستغلونها، كانت الأفكار المثيرة للقلق تصفع وترهب بضعة محللين داخل وكالة الأمن القومي: إن أي شيء نفعله بهم، باستطاعتهم أن يفعلوه بنا.

تعمَّق هذا القلق بعد أن شرع عدد متزايد من المؤسسات، والمرافق العمومية، ومقاولي الحكومة في البدء بتخزين بياناتهم وإدارة عملياتهم على حواسيب مؤللة، لا سيما أن بعضهم كان يمزج البيانات المصنفة على أنها سرية مع البيانات غير السرية على جهاز واحد، وحتى في برمجية واحدة. إن تحذيرات ويليس وير التي أطلقها قبل ذلك بنحو اثني عشر عاما كانت تنبئية وتنذر بالخطر.

لم يكن كل شخص في وكالة الأمن القومي يشعر بالانزعاج. كان هناك رضا عن الذات، وانتشار للتهاون والتقاعس بشأن الاتحاد السوفييتي. كان هناك ارتياب، بل حتى سخرية من فكرة أن دولة متخلفة جدا من الناحية التكنولوجية، كان يمكنها أن تفعل الأشياء الباهرة التي تضطلع بها فرق استخبارات الإشارات الأمريكية. إضافة إلى ذلك فإن مديري وكالة الأمن القومي كانوا غير راغبين ومترددين في إصلاح الفجوات الأمنية الموجودة في الحواسيب والبرمجيات. كان الكثير من هذه الأجهزة والبرمجيات يُستخدم (أو يُنسخ) في دول عدة بكل أرجاء العالم، بمن في ذلك المستهدفون برصد وكالة الأمن القومي؛ فإذا كان من السهل اختراقها، كان ذلك أفضل للمراقبة.

كان لدى وكالة الأمن القومي مديريتان رئيسيتان: «استخبارات الإشارة» (سيجينت) Signals Intelligence (SIGINT) و«أمن المعلومات» (إنفوسك) Information Security (INFOSEC) (أصبحت في وقت لاحق تسمى «ضمان المعلومات» Information Assurance). كانت مديرية استخبارات الإشارات هي الجانب النشط والمشرق من قصر الأحاجي، حيث المهندسون، وخبراء تشفير، وجواسيس المدرسة القديمة، يجرفون ويتفحصون البث الراديوي (اللاسلكي)، ويتنصتون على الدوائر والكابلات. وكان كل هذا بهدف اعتراض وتحليل الاتصالات التي تؤثر في الأمن القومي. أما مديرية أمن المعلومات (إنفوسك)، فقد كانت تختبر موثوقية وأمن الأجهزة والبرمجيات التي كانت فرق استخبارات الإشارات تستخدمها. لكن على مدار

معظم تاريخ الوكالة لم يكن هناك اتصال مباشر بين الجانبين وحتى لم يكن يضمهما بناية واحدة. إن معظم وكالة الأمن القومي، بما في ذلك مديرية استخبارات الإشارة (سيجينت)، كانت تعمل في مجمع ضخم يقع في منشأة «فورت ميد» العسكرية بولاية ماريلاند. أما مديرية أمن المعلومات (إنفوسك)، فقد كانت تبعد عشرين دقيقة بالسيارة، في بناية من الطوب البني قاتم اللون تسمى «فانيكس» FANEX ملحقة بمطار «فريندشيب» (الصداقة) Friendship Airport، الذي أصبح فيما بعد يعرف بمطار «بي دبليو آي مارشال» BWI Marshall. (حتى العام 1968 كانت مديرية أمن المعلومات (إنفوسك) أبعد من ذلك، في بناية منزوية - صارت بعد ذلك بعدة أعوام مقرا لوزارة الأمن الداخلي - تقع على «طريق نبراسكا» Nebraska Avenue، في شمال غرب واشنطن). لقد كانت أعمال الصيانة هي مهمة تقنيي مديرية أمن المعلومات، ولم يكونوا قط جزءا من العمليات. أما فرق استخبارات الإشارات فلم يكونوا يفعلون شيئا سوى العمليات، ولم يكونوا يتشاركون ملكاتهم أو فراستهم وأفكارهم الثاقبة للمساعدة على إصلاح ما كانوا يرصدونه من عيوب في المعدات.

بدأ هذان الكيانان في توحيد قواهما بعض الشيء مع اقتراب نهاية فترة رئاسة كارتر. تزايد إدراك مسؤولي البنتاغون أن السوفييت كانوا ينفذون إلى روابط اتصالاتهم، ورغبوا في أن تبدأ مديرية أمن المعلومات (إنفوسك) في اختبار الأجهزة والبرمجيات المستخدمة ليس فقط لدى وكالة الأمن القومي، ولكن لدى وزارة الدفاع بصفة عامة. أنشأ إنمان مؤسسة جديدة، أطلق عليها اسم «مركز أمن الحاسوب» (Computer Security Center)، وطلب من جورج كوتر George Cotter، مدير العلوم والتكنولوجيا لديه، أن يتولى إدارة المركز. كان كوتر واحدا من أفضل خبراء التشفير في البلاد. كان يعمل في استخبارات الإشارات منذ نهاية الحرب العالمية الثانية، وقد عمل لدى وكالة الأمن القومي منذ إنشائها. أراد إنمان أن يبدأ المركز الجديد في دمج مسؤولي العمليات في مديرية استخبارات الإشارة (سيجينت) مع التقنيين في مديرية أمن المعلومات (إنفوسك) في مشروعات مشتركة. كانت الثقافات ستبقى مستقلة ومختلفة لأعوام تالية، لكن الحواجز بدأت تتراجع وتزول.

جاء الأمر بإنشاء «مركز أمن الحاسوب» من مساعد وزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات (إيه إس دي «سي3 آي» - ASD

«C3I»)، وهو حلقة الوصل بين البنتاغون ووكالة الأمن القومي. وحينما صار ريغان رئيسا، عيَّن وزير دفاعه كاسبار واينبرجر Caspar Weinberger دونالد لثام Donald Latham في هذا المنصب. كان لثام قد أدار مشروعات تابعة لمديرية استخبارات الإشارة (سيجينت) مع جورج كوتر خلال النصف الأول من سبعينيات القرن العشرين على الخطوط الأمامية لجبهة الحرب الباردة، لثام بوصفه كبير علماء قيادة الولايات المتحدة في أوروبا، وكوتر بوصفه نائب رئيس وكالة الأمن القومي في أوروبا. مثل أي شخص وثيق الصلة كان كل منهما يعلم تماما مدى عمق وصول كل من الجانبين - السوفييت والأمريكان (وأيضا بعض حلفائهما الأوروبيين) – إلى داخل قنوات اتصال الآخر. بعد أن ترك لثام وكالة الأمن القومي رُشِّح نائبا لرئيس مكتب البنتاغون لأنظمة الموجات الميكروية (ميكروويف)، والفضائية، والجوالة. ومن هناك، استمر في شغل مناصب هندسية عليا في شركة «مارتن ماريتا» Martin Marietta(*) ومؤسسة «أر سي إيه» RCA(**)، حيث ظل مستغرقا في تلك القضايا.

عندما عاد الجنرال جاك فيسي من ذلك الاجتماع في البيت الأبيض بعد أن كان رونالد ريغان قد شاهد فيلم «ألعاب الحرب (المناورات الحربية)» وطلب من معاونيه معرفة ما إذا كان يمكن لأحد أن يخترق الحواسيب الأكثر حساسية، كان من الطبيعي أن يحوِّل موظفوه السؤال إلى دون لثام. لم يستغرق الأمر من لثام وقتا طويلا ليرسل ردا، الإجابة ذاتها التي كان فيسي سيقدمها إلى الرئيس: نعم، المسألة أسوأ كثيرا مما تظن.

(*) كانت مارتن ماريتا Martin Marietta هي إحدى الشركات الأمريكية، أُسست في العام 1961 من خلال اندماج شركتي «جلين إل مارتن» Glenn L. Martin Company و«أمريكان ماريتا» American-Marietta Corporation. أصبحت الشركة المندمجة رائدة في الصناعات الكيميائية، والفضائية، والإلكترونيات. في العام 1995 اندمجت مع مؤسسة «لوكهيد» Lockheed لتشكيل شركة «لوكهيد مارتن» Lockheed Martin. [المترجم]

(**) مؤسسة «أر سي إيه» RCA، هي شركة إلكترونيات أمريكية كبرى أُسست في العام 1919، كانت في البداية شركة تابعة مملوكة بالكامل لشركة «جنرال إلكتريك» General Electric (GE)، غير أنه في العام 1932 كان مطلوبا من «جنرال إلكتريك» رفع سيطرتها باعتبار ذلك جزءا من تسوية دعوى قضائية حكومية لمكافحة الاحتكار. كانت «أر سي إيه» في أوجها كشركة مستقلة هي شركة الاتصالات السائدة في الولايات المتحدة لأكثر من خمسة عقود، وبدءا من أوائل عشرينيات القرن العشرين، كانت «أر سي إيه» مصنعا رئيسيا لأجهزة الاستقبال اللاسلكية، كما أنشأت أول شبكة إذاعية وطنية، وكانت أيضا في طليعة مقدمي ومطوري التلفاز، سواء الأبيض والأسود أو الملون. حاليا تمتلك شركة «سوني ميوزيك إنترتاينمنت» Sony Music Entertainment وشركة «تكنيكولور» Technicolor علامات «أر سي إيه» التجارية، ومُنحتا ترخيص اسم العلامة التجارية لمنتجاتها المختلفة لشركات أخرى. [المترجم]

كان لثام قد كلف بالعمل على التوجيه الرئاسي المسمى «إن إس دي دي - 145» (التوجيه الرئاسي السري المتعلق بالأمن القومي)، وفي نهاية المطاف إعداد مسودة التوجيه الرئاسي. كان لثام يعرف الأساليب المختلفة التي كانت وكالة الأمن القومي - وكالة الأمن القومي فقط من بين جميع الدوائر الفدرالية - تستطيع بها ليس فقط اختراق الاتصالات والحواسيب، بل تأمينها أيضا. لذلك وضع في مسودته أن تكون وكالة الأمن القومي مسؤولة عن كل وسائل تأمينها.

دعا التوجيه إلى إنشاء لجنة قومية لأمن أنظمة الاتصالات والمعلومات «للنظر في المسائل التقنية» و«وضع سياسات تشغيلية» لتطبيق السياسة الجديدة. كان مساعد وزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات (إيه إس دي «سي3 آي») هو الذي سيتولى رئاسة اللجنة، وكان هذا يعني أن دون لثام سيكون رئيسا لها.

أيضا نص التوجيه على أن تشتمل اللجنة على «أمانة دائمة تتألف من عناصر من وكالة الأمن القومي»، وهذه الأمانة «ستقدم التسهيلات والدعم وفق الحاجة». كما سيكون هناك «مدير قومي للاتصالات وأمن أنظمة المعلومات المؤللة»، الذي كان سيضطلع «بمراجعة واعتماد كل المعايير، والتقنيات، والأنظمة، والمعدات». حدد التوجيه أن يتولى مدير وكالة الأمن القومي منصب المدير القومي.

كان برنامجا طموحا، وبالنسبة إلى البعض، فإنه كان طموحا جدا. إن عضو الكونغرس جاك بروكس Jack Brooks، العضو الديموقراطي عن ولاية تكساس Texas، وكبير المدافعين عن الحريات المدنية في «الكابيتول هيل» Capitol Hill (الكونغرس)، لم يكن ليسمح لوكالة الأمن القومي بأن تؤدي أي دور في الحياة اليومية للأمريكيين، تلك الوكالة التي كانت أعمالها بموجب الدستور تنحصر في مراقبة الأجانب. كتب جاك بروكس مشروعا لقانون لمراجعة وتنقيح التوجيه الرئاسي، وأقره زملاؤه من المشرعين، وحرمت الوكالة من أيٍ من مثل هذا النفوذ. لو كانت الصياغة اللغوية لعبارات دون لثام قد تُركت كما هيَ، لكانت المعايير الأمنية وتوافق والتزام كل حاسوب في أمريكا - في الحكومة، وفي الأعمال، والحواسيب الشخصية - كانت ستوضع تحت تفرس وكالة الأمن القومي الدؤوب الذي لا يعرف الكلل.

لم تكن هذه هي المرة الأخيرة التي تحاول فيها الوكالة فرض هذه السلطة وبسط هذا النفوذ، أو أن يضطلع أحد آخر بالتصدي لها وإبعادها.

2

«الأمر كله يتعلق بالمعلومات»

في 2 أغسطس 1990، أمر الرئيس العراقي صدام حسين جيشه بغزو الكويت. وبعد مضي ثلاثة أيام، أعلن الرئيس جورج دبليو بوش (الأب) George H. W. Bush أن هذا العدوان «لن يستمر». في 17 يناير 1991، وبعد تعبئة ضخمة، أطلقت المروحيات والطائرات المقاتلة الأمريكية أولى طلقات الحملة الجوية على العراق التي دامت شهرا، أعقبها هجوم بري في 24 فبراير دام 100 ساعة، وشارك فيه أكثر من نصف مليون جندي أمريكي، طوق الجيش العراقي وسحقه، ودفع الناجين المتناثرين إلى العودة عبر الحدود.

عُرفت تلك العملية باسم «عاصفة الصحراء»، وكانت أكبر هجوم مدرع شهده العالم منذ الحرب العالمية الثانية. وكانت أيضا – على الرغم من قلة من كان على علم بذلك

«كانت عملية عاصفة الصحراء هي الحملة الأولى لوسائل الحرب المضادة للقيادة والسيطرة التي تنذر بمجيء حروب سيبرانية»

– هي الحملة الأولى لوسائل الحرب المضادة للقيادة والسيطرة التي تنذر بمجيء حروب سيبرانية.

في ذلك الوقت، كان مدير وكالة الأمن القومي هو الأدميرال (لواء بحري) وليام ستوديمان William Studeman، الذي كان مديرا لاستخبارات سلاح البحرية قبل توليه القيادة في «فورت ميد»، مثل معلمه ومرْشده بوبي راي إنمان. حينما عُين ستوديمان لإدارة وكالة الأمن القومي، أخذ معه خبيرا مخضرما ومتمرسا في التشْفير من سلاح البحرية يدعى ريتشارد ويلهلم Richard Wilhelm، واتخذه مساعدا تنفيذيا له. قبل ذلك ببضعة أعوام، كان ويلهلم هو الرجل الثاني في أحد أكبر مواقع الوكالة لاستخبارات الإشارة (سيجينت) في قرية إدزل Edsall في أسكتلندا، حيث كان يدير منصة اختبار برنامج «إنمان» لترقية كفاءة الإشارات المرمزة (بي إس يو)، الذي كان يهدف إلى فك تشْفير الاتصالات السوفييتية.

مع بدء التخطيط لعملية «عاصفة الصحراء»، أوفد ستوديمان ويلهلم إلى البنتاغون بوصفه مفوض وكالة الأمن القومي لمجموعة كُونت في عجالة ومن دون سابق إعْداد، أطلق عليها اسم «مركز الاستخبارات المشتركة» Joint Intelligence Center. كان رئيس ذلك المركز هو الأدميرال (لواء بحري) جون «مايك» ماكونيل John «Mike» McConnell، الذي كان يشغل منصب «جيه - 2 J-2»، ضابط الاستخبارات لرئيس الهيئة المشتركة لرؤساء الأركان. مثل معظم الضباط سريعي الترقي في استخبارات سلاح البحرية، كان ويلهلم وماكونيل قد عرف كل منهما الآخر طوال أعوام. في ذلك المركز الجديد، أنشآ جهازا متعدد الأفرع يجمع بين استخبارات الإشارة (سيجينت)، والتصوير بالأقمار الاصطناعية، والجواسيس البشريين الميدانيين، تضمهم خلية واحدة لجمع المعلومات الاستخباراتية وتحليلها.

قبل الغزو، لم يكن ضباط الاستخبارات الأمريكية يعرفون الكثير عن العراق أو عن آلة صدام حسين العسكرية. بحلول موعد القصف، كانوا قد عرفوا معظم ما كانت تلزم معرفته. قبل أشهر من إطلاق الطلقة الأولى، نفذ محللو ماكونيل إلى عمق شبكة صدام للقيادة والسيطرة، وكان أهم ما اكتشفوه، هو أن صدام كان قد مد كابل ألياف ضوئية على طول الطريق من بغداد إلى البصرة، وبعد غزوه الكويت، مده إلى مدينة الكويت. اتصل ضباط الاستخبارات الأمريكيون بالشركات

الغربية التي ركّبت الكابل، وعلموا منهم مواقع أنظمة التبديل. حينما بدأ القصف في الساعات الأولى من يوم 17 يناير، كانت تلك المبدلات من بين الأهداف الأولى التي دُمرت. كان على صدّام أن يعيد توجيه الاتصالات إلى شبكته الاحتياطية، التي كانت تعتمد على إشارات الموجات الميكروية (ميكروويف). استباقا لهذه الخطوة، كانت وكالة الأمن القومي قد وضعت قمرا اصطناعيا سريا جديدا فوق العراق مباشرة، وهو أحد ثلاثة أنظمة للتجسس في السماء كان ويلهلم قد تمكّن من تدبيرها قبل الحرب. كان هذا القمر الاصطناعي يحمل جهاز استقبال يمكنه تفحص إشارات الموجات الميكروية (ميكروويف).

من ثم، فإن وكالة الأمن القومي، ومركز الاستخبارات المشتركة الذي يترأسه ماكونيل، ومن خلالهما القادة العسكريون الأمريكيون، كانوا في كل خطوة يعرفون تماما ما الذي كان يقوله صدام وجنرالاته، وتحركات جنودهم. نتيجة لذلك، اكتسبت الولايات المتحدة أفضلية هائلة في المعركة، لم تقتصر على أن قادتها كان في استطاعتهم التصدي بسرعة خاطفة لتحركات الجيش العراقي، بل كان في استطاعتهم أيضا تحريك قواتهم في الأرجاء من دون أن يخشوا اكتشافها. كان لدى العراقيين الكثير من الصواريخ المضادة للطائرات، التي كانوا قد حصلوا عليها من السوفييت على مر الأعوام، وكانوا مدربين جيدا على استخدامها. ربما كانوا سيسقطون مزيدا من الطائرات المقاتلة الأمريكية، لكن المركز الذي أنشأه ماكونيل اكتشف كيفية تعطيل أنظمة القيادة والسيطرة العراقية ورادارات دفاعاتهم الجوية.

سرعان ما اكتشف ضباط استخبارات صدام ما حدث من انتهاك، فبدأوا بإرسال الأوامر إلى الجبهة عبر سعاة يستقلون دراجات نارية. لكن هذه العملية كانت بطيئة، وكانت الحرب آنذاك تتحرك سريعا، ولم يكن هناك الكثير الذي يستطيع صدّام فعله لتفادي الهزيمة.

كانت هذه التجربة الأولى لوسائل الحرب المضادة للقيادة والسيطرة تجربة ناجحة، لكنها لم تتقدم أبعد من ذلك كثيرا، ليس بقدر ما كان يستطيع مناصروها تحقيقه، وذلك لأن الأمر لم يكن في دائرة اهتمام كبار ضباط الجيش الميداني (القوات البرية) للولايات المتحدة. كان الجنرال نورمان شوارتزكوف Norman Schwarzkopf، قائد عاصفة الصحراء المختال، رافضا على نحو استثنائي. كان

قائد «عاصفة الصحراء» ينتمي إلى المدرسة القديمة، ويؤمن بأن كسب الحروب يتحقق عن طريق قتل العدو وتدمير أهدافه، وفي هذا السياق، فإن جميع الحروب متشابهة، كبيرة أو صغيرة، تقليدية أو حرب عصابات، على تلال أوروبا المنحدرة، أو في أدغال فيتنام، أو عبر صحارى بلاد ما بين النهرين (بلاد الرافدين).

في الأساس، لم يكن شوارتزكوف يرغب في أن تكون له أي علاقة بالمعلومات التي ترد من مركز ماكونيل. لم يكن قد أحضر معه سوى حفنة من ضباط الاستخبارات، معتقدا أنهم كانوا سيسدون حاجة المهمة. أثار هذا الأمر احتجاج الأوساط الاستخباراتية بأسرها، كمديري وكالة الاستخبارات المركزية، ووكالة الأمن القومي، ووكالة استخبارات الدفاع، وغيرهم. تطلب الأمر تدخل رئيس الهيئة المشتركة لرؤساء الأركان، كولين باول Colin Powell، وهو جنرال في الجيش الميداني (القوات البرية) له الهيئة والمنظور الاستراتيجي الذي يتسم به المشتغلون بالسياسة في العاصمة واشنطن، ودعا محللي المعلومات الاستخباراتية في المركز إلى الحوار مع مخططي الحرب.

مع ذلك، أبدى شوارتزكوف ممانعة. حينما علم أن صدّام كان ينقل أوامره عن طريق الموجات الميكروية (ميكروويف) بعد تدمير كابلات الألياف الضوئية، كان حدسه الأول هو نسف وصلة الموجات الميكروية (ميكروويف). عارضه بعض من محللي المعلومات الاستخباراتية في فريقه، محتجين بالكم الهائل من المعلومات الثمينة التي كانوا يحصلون عليها من اعتراض تلك الوصلات. رفض شوارتزكوف تلك الدفوع، وأصر على أن تدمير روابط اتصال صدام، بدلا من استغلالها في الاستخبارات، سيكون هو الطريق الأسرع نحو النصر.

لم يكن شوارتزكوف فقط هو الذي ألغى مخططات «مركز الاستخبارات المشتركة». كان كبار مسؤولي البنتاغون المدنيين (غير العسكريين) هم أيضا مرتابين، لقد كان كل هذا جديدا جدا. كان القليل من السياسيين أو كبار المسؤولين على دراية بالتكنولوجيا، ولم يكن أي من الرئيس بوش أو وزير دفاعه ديك تشيني Dick Cheney قد استخدم حاسوبا من قبل مطلقا. عند نقطة حاسمة في الحرب، بينما كانت القوات البرية الأمريكية تعد خطواتها النهائية لمهاجمة الجيش العراقي من الجناحين ومن الخلف، اقترحت وكالة الأمن القومي ومركز الاستخبارات المشتركة تعطيل أحد أبراج الاتصالات العراقية عن طريق اختراق مكوناته الإلكترونية. كان

المطلوب هو وضع البرج خارج الخدمة مدة أربع وعشرين ساعة فقط. لم تكن هناك حاجة إلى تفجيره، إذ إنه من المحتمل قتل بعض أناس أبرياء في أثناء ذلك. كان تشيني متشككا، وسأل المحللين عن مدى ثقتهم بنجاح الخطة؛ كانوا غير قادرين على تحديد كم الصعاب وأرجحية العملية. على النقيض من ذلك، كان إسقاط بعض القنابل من الطائرات المقاتلة سينجز المهمة على نحو قاطع. اختار تشيني القنابل.

خرج أولئك الذين كانوا مستغرقين في الجانب السري للحرب المضادة للقيادة والسيطرة من المعركة ولديهم شعور بزهو الانتصار، لكن البعض شعر أيضا بالحيرة والانزعاج. قبل بدء القتال، كان ريتشارد إتش إل مارشال Richard H. L. Marshall، المستشار القانوني لوكالة الأمن القومي، قد أعرب عن بعض المخاوف بشأن خطة المعركة. عند مرحلة ما، كان من المفترض استخدام وسائل إلكترونية لتعطيل أحد مولدات الكهرباء العراقية، الذي كان يمد إحدى المنشآت العسكرية بالطاقة. لكن مارشال رأى أن المولد يمد أيضا أحد المستشفيات القريبة بالطاقة اللازمة لتشغيلها. كان هناك احتمال أن هذا الهجوم – على الرغم من أنه لم يتضمن رصاصات، أو صواريخ، أو قنابل – سيقتل كثيرا من المدنيين، بل وأكثر المدنيين عجزا.

عقد مارشال ومحامون آخرون في وكالة الأمن القومي والبنتاغون، نقاشا ساخنا بشأن الآثار المترتبة على ذلك الهجوم. ثبت أن مخاوفهم كانت محل جدل وغير ذات موضوع، قرر شوارتزكوف وغيره من القادة إسقاط القنابل والصواريخ على مولد الكهرباء وتقريبا على كل هدف مدني آخر، مثل: محطات توليد الطاقة، ومراكز تنقية المياه، وأبراج الاتصالات، ومختلف المرافق ذات الوظائف المدنية والعسكرية المزدوجة. وسبب «الضرر المصاحب» قتل آلاف المدنيين العراقيين.

مع ذلك، ومن موقعه المتميز في وكالة الأمن القومي، كان مارشال يستطيع أن يتوقع طفرة نمو في هذا النوع الجديد من وسائل الحرب، ربما في وقت ما في المستقبل غير البعيد، حينما تصل تلك الوسائل إلى مرحلة النضج لتصير نمطا سائدا من وسائل الحرب. إذا قامت دولة بتدمير أو إعاقة جزء من البنية الأساسية (المرافق العامة) الحرجة، من دون إطلاق قذيفة أو إسقاط قنبلة، فهل كان ذلك سيعد بمنزلة عمل من أعمال الحرب؟ هل كان سيخضع قادتها ومقاتلوها لـ «قانون النزاع

المسلح»(*) Law of Armed Conflict؟ لم يكن أحد يعرف، لم يكن أي أحد ممن لديه سلطة مناقشة مثل هذه الأمور قد فكر في ذلك مطلقا.

ثمة ضباط آخرون رفيعو المستوى في وكالة الأمن القومي، من ذوي التوجه العملياتي، كان لديهم اهتمام مختلف، وأكثر استراتيجية. كانوا مشدوهين من مدى السهولة التي جرى بها تعطيل روابط اتصالات صدّام. لكن البعض كان يعرف أنه في حرب مستقبلية، لا سيما في مواجهة عدو أكثر تقدما من العراق، ربما لا يكون الأمر يسيرا هكذا. كانت التكنولوجيا تتغير، من التماثلية (التناظرية) إلى الرقمية، من البث الراديوي (اللاسلكي) والموجات الميكروية إلى الألياف الضوئية، من «الدوائر المنفصلة» (المستقلة) discrete circuits لخطوط الهاتف إلى «حزم البيانات» data packets لما كان سيُطلق عليه اسم «الفضاء السيبراني». حتى صدّام حسين كان لديه كابل ألياف ضوئية، ولأن حلفاء أوروبيين هم الذين كانوا قد ركّبوها، كان في استطاعة المسؤولين الأمريكيين معرفة موضع المبدلات، ومن ثم معرفة مكان إسقاط القنابل. لكن كان يمكن للمرء أن يتخيل دولة معادية أخرى تمد كابلها بنفسها؛ أو، إذا لم تكن هناك حرب، إذا رغبت وكالة الأمن القومي ببساطة في اعتراض الإشارات التي تطِّن عبر الكابل، تماما مثلما ظلت طويلا تعترض الاتصالات الهاتفية والبث الراديوي (اللاسلكي)، فلن يكون هناك سبيل للولوج. ربما يكون من الممكن تقنيا التنصت على الكابل، ولكن وكالة الأمن القومي لم تكن مهيأة لهذه المهمة.

كان المسؤول الأكثر قلقا بشأن هذه الاتجاهات هو مدير وكالة الأمن القومي بيل ستوديمان.

في أغسطس 1988، قبل أيام قليلة من تولي ستوديمان القيادة في «فورت ميد»، دعاه إنمان إلى تناول العشاء، ودعا زميلا قديما آخر، هو ريتشارد هافر Richard Haver. كانت سبعة أعوام قد مرت منذ تولي إنمان إدارة وكالة الأمن القومي، وهو لم يكن راضيا عما كان قد فعله في المكان خليفتاه – لنكولن فاورير Lincoln

(*) نشأ قانون النزاع المسلح عن رغبة الدول المتحضرة في منع المعاناة والدمار غير الضروريين، وبما لا يعوق شن الحرب على نحو فعال، وهو جزء من القانون الدولي العام، وينظم سلوك الأعمال القتالية المسلحة. كما يهدف قانون النزاع المسلح إلى حماية المدنيين، وأسرى الحرب، والجرحى، والمرضى، والغرقى. ينطبق قانون النزاع المسلح على النزاعات المسلحة الدولية، وفي تنفيذ العمليات العسكرية، والأنشطة ذات الصلة في النزاعات المسلحة، أيا كان توصيف هذه الصراعات. [المترجم].

Faurer ووليام أودوم William Odom. كلاهما كان جنرالا من فئة النجوم الثلاثة، كان فاورير من سلاح الجو، وكان أودوم من الجيش الميداني (القوات البرية) (عادة ما كان منصب المدير بالتناوب بين الفروع)، وبالنسبة إلى إنمان، رجل سلاح البحرية، كان هذا جزءا من المشكلة.

من بين الفروع العسكرية الثلاثة الرئيسية، كان سلاح البحرية هو الأكثر مواكبة للتغيرات الحادثة في تكنولوجيا الاستطلاع. كانت مهمته رقم واحد[1] هي تتبع الأسطول السوفييتي، لا سيما الغواصات السوفييتية. وكان أحد الفروع الأكثر سرية في سلاح البحرية الأمريكي هو الذي يضطلع بهذه المطاردة مستخدما عديدا من الأدوات والتقنيات ذاتها التي كانت وكالة الأمن القومي تستخدمها. كانت هناك روح جماعية تسود بين زمرة ضباط سلاح البحرية الذين ارتقوا المراتب في صفوف تلك البرامج فائقة السرية. كان هذا من ناحية يرجع إلى أنهم كانوا رفيعي المستوى جدا، كونهم لديهم التصريح لمعرفة أدق التفاصيل عن تلك البرامج مما جعلهم أعضاء في العصبة العسكرية الأكثر سرية. من ناحية أخرى، نبعت تلك الروح الجماعية من ضراوة مهمتهم، إذ إن ما كانوا يفعلونه في وقت السلم، على مدار الساعة وطوال أيام الأسبوع، من كسر لرموز الشفرات السوفييتية، ومطاردة الغواصات السوفييتية، كان إلى حد كبير هو الأشياء ذاتها التي كانوا سيفعلونها في وقت الحرب. كان الشعور بالاستعجال والضرورة الملحة لا يهدأ أبدا.

في نهاية المطاف، كانت روح الانتماء هذه التزاما ابتدعه بوبي راي إنمان. حينما كان مديرا لاستخبارات سلاح البحرية في منتصف السبعينيات من القرن العشرين، ساعده كبير معاونيه على تحديد أمهر الرجال في مختلف فروع سلاح البحرية - الملحقين، والضباط على حاملات الطائرات، بالإضافة إلى غواصي العمليات الخاصة وخبراء الشفرة - ووضعهم معا في فرق، للتأكد من أن المعلومات الاستخباراتية الأكثر أهمية قد وصلت إلى أيدي رجال العمليات، وأن مهمات رجال العمليات تتسق مع احتياجات ضباط الاستخبارات.

كان إنمان منفذا شرسا للسياسات البيروقراطية، وكان بيل ستوديمان وريتشارد هافر يروق لهما القول إن مكيافيللي كان ملاكا مقارنة به. في أواخر السبعينيات وأوائل الثمانينيات من القرن العشرين، وباعتباره مديرا لوكالة الأمن القومي، انشغل

إنمان في صراعات مطولة بشأن السلطة بشأن أي من الوكالتين - وكالة الأمن القومي أو وكالة الاستخبارات المركزية - هي التي ستسيطر على التكنولوجيات الجديدة. حينما انتُخب رونالد ريغان رئيسا، كانت فترة ولاية إنمان باعتباره مديرا لوكالة الأمن القومي قد شارفت على الانتهاء، وطلب منه ريغان الانتقال إلى لانجلي Langley ليصير نائبا لمدير وكالة الاستخبارات المركزية. كان مجلس الشيوخ قد صدّق على ترشيحه للوظيفة الجديدة في 12 فبراير 1981، لكنه ظل مديرا لوكالة الأمن القومي حتى 30 مارس. في تلك الفترة من الصلاحيات المزدوجة التي استغرقت ستة أسابيع، أرسل إنمان عدة مذكرات إلى نفسه، من مدير وكالة الأمن القومي إلى نائب مدير وكالة الاستخبارات المركزية، والعكس بالعكس، ومن ثم أجرى تسوية وحل العديد من المسائل بين الوكالتين. (كان رئيس إنمان في وكالة الاستخبارات المركزية هو مديرها وليام كايسي William Casey، الذي كان جل تركيزه ينصب على الحروب السرية ضد الشيوعيين في أمريكا الوسطى وأفغانستان، لذا لم يكن يكترث بالأمور الداخلية). في النهاية، انفردت وكالة الأمن القومي بالسيطرة على الاستخبارات المعتمدة على الحاسوب (مهّد ذلك الساحة، بعد ثلاثة أعوام، للتوجيه الرئاسي السري المتعلق بالأمن القومي «إن إس دي دي145- NSDD-145» الذي أصدره ريغان، والذي أعطى وكالة الأمن القومي سلطة وضع معايير أمنية لكل الاتصالات والحواسيب، إلى أن ألغاها الكونغرس. كانت مذكرات إنمان التي تبادلها مع نفسه قد أرست سوابق هذه السلطة. في بضعة خلافات أخرى، فصل إنمان وقسّم المسؤوليات، وأنشأ فرقا مشتركة بين وكالة الاستخبارات المركزية ووكالة الأمن القومي. أيضا، وبفضل تأمين الأدوار والمهمات، عزز إنمان موازنات الوكالتين من أجل الأجهزة باهظة الثمن التي كان قد رغب في الحصول عليها في «فورت ميد»، بما في ذلك الحواسيب الفائقة، والرقائق المصغرة التي تحسّن القدرات التجميعية لمستشعرات الأقمار الاصطناعية، وطائرات التجسس، والغواصات.

بقي «إنمان» في وكالة الاستخبارات المركزية أقل من عامين، ثم تقاعد من الحكومة، وعاد إلى مسقط رأسه في ولاية تكساس، وحقق ثروة من إنشاء شركات برمجيات وشركات التشْفير للأغراض التجارية. من هذا الموضع المتميز، رأى إنمان الكيفية التي كانت تنتشر الثورة الرقمية من خلالها سريعا في كل أرجاء العالم، والكيفية التي كان سيتعين بها على وكالة الأمن القومي أن تتغير بشكل جذري لمواكبة ذلك التقدم. ظل

إنمان فاعلا في المجالس الاستشارية الحكومية، ويتواصل من حين إلى آخر مع مرؤوسيه السابقين في «فورت ميد»، وكان قد أصيب بالإحباط لأن لنكولن فاورير، ثم ويليام أودوم، لم يهتما بالمنعطفات الحادة والتغيرات الهائلة المقبلة.

وفي العام الأخير من فترة رئاسة ريغان، كان بيل ستوديمان، الذي لم يكن فقط رجل سلاح البحرية ذا الخبرة في المشروعات السرية، بل هو أيضا صِنْو من تكساس وأحد تلاميذ إنمان المفضّلين، على وشك أن يصير مديرا لوكالة الأمن القومي. أما ريتشارد هافر، الذي انضم إلى الاثنين لتناول العشاء في تلك الليلة الصيفية، فكان هو نائب مدير الاستخبارات البحرية.

حينما كان إنمان مديرا للاستخبارات البحرية، كان ستوديمان وهافر قد عملا ضمن فريقه. كان ستوديمان قد عمل على أوجه التقدم في الاستطلاع والمعالجة الحاسوبية، بما في ذلك برنامج «ترقية كفاءة الإشارات المرمزة (بي إس يو)»، الأمر الذي منح أمريكا أفضلية على روسيا في بداية رئاسة ريغان. أما هافر، وهو شخصية مقنعة في العروض التقديمية، فكان هو الذي أحاط الرئيس وكبار معاونيه علما بالآثار المترتبة على أوجه التقدم. كان ثلاثتهم - إنمان، وستوديمان، وهافر - حاصلين على شهادات في التاريخ، وليس في الفيزياء أو الهندسة. كان العالم يتغير، كانت الحرب الباردة تدخل إلى مرحلة جديدة، وهم كانوا يرون أنفسهم عناصر فاعلة على خط المجابهة في عالم النضال الذي غالبا لم يكن أحد غيرهم يعرفه.

كان إنمان قد دعا مرؤوسيه السابقين الاثنين معا في تلك الليلة ليخبرهما بأنه كان يجب عليهما دفع أوساط الاستخبارات، لا سيما وكالة الأمن القومي، في مواجهة التغيرات التكنولوجية، هو بالأحرى دعاهما ليلقي عليهما محاضرته، طوال فترة تناول العشاء التي استغرقت ثلاث ساعات كاملة. كان على ستوديمان، وهافر تغيير أسلوب عمل الوكالات، والنهوض بأفرادها، وتركيز طاقاتهم.

بعد ذلك ببضعة أيام، تولى ستوديمان دفة القيادة في فورت ميد، وكان من بين الأشياء الأولى التي أنجزها الأمر بإعداد بحثين، أحدهما أطلق عليه «دراسة إمكانية الوصول العالمي» (العمومي) Global Access Study، تناول الكيفية التي سيتحول بها العالم سريعا من التماثلية (التناظرية) إلى الرقمية. خلص البحث إلى أن التغيير لم يكن ليحدث دفعة واحدة أو على نحو متجانس، وأن وكالة الأمن القومي كان

عليها الابتكار لكي تلبي مقتضيات العالم الجديد (وتعترض الاتصالات)، فيما تستمر في رصد المشهد الراهن لإشارات الهاتف، والإشارات الراديوية (اللاسلكية)، وإشارات الموجات الميكروية.

أما بحث ستوديمان الثاني، الذي تناول تحليلا لموظفي وكالة الأمن القومي ومجموعات مهاراتهم، فقد خَلَص إلى أن التوازن كان خطأً، فقد كان هناك عدد كبير جدا من الخبراء في شؤون الكرملين، وليس هناك ما يكفي من خبراء الحاسوب. حينما كان إنمان مديرا كان قد اتخذ بضع خطوات صغيرة لجمع التقنيين مع رجال العمليات ومحللي استخبارات الإشارة (سيجينت) في غرفة واحدة، لكن المساعي كانت قد توقفت منذ ذلك الحين. كان معظم خبراء الحاسوب في الوكالة يعملون في مجال تكنولوجيا المعلومات أو الصيانة. لم يكن أحد في استخبارات الإشارة (سيجينت) يستفيد من خبراتهم للحصول على المشورة بشأن نقاط الضعف والثغرات الأمنية في المعدات والبرمجيات الجديدة. باختصار لم يكن أحد يستعد للحقبة الجديدة.

أدت دراسات ستوديمان - التي كان هو في الحقيقة الذي أعدها - إلى اشتعال معارضة، وغضب، وخوف لدى الجميع بلا استثناء. كان مديرو وكالة الأمن القومي على مر الأعوام قد استثمروا - وكانوا مستمرين في أن ينفقوا - مبالغ هائلة على التكنولوجيا التماثلية (التناظرية)، واختاروا أن يتجاهلوا أو يرفضوا تحذيرات بأنهم كانوا قد اتخذوا رهانا خاسرا. أخذ الحرس القديم دراسة ستوديمان الثانية، الدراسة التي كانت تنذر بعدم التوافق الوشيك بين مجموعات مهارات الوكالة ومهامها، على أنها على وجه الخصوص تنذر بخطر مشؤوم، وإذا اتخذ المدير الجديد إجراءات بناء على نتائج دراسته، فإن الآلاف من المحللين والجواسيس المخضرمين سيصبحون عما قريب بلا عمل.

كان هذا هو أقصى ما يستطيع ستوديمان فعله خلال الأعوام الثلاثة التي قضاها في موقع المسؤولية، لأمر واحد، هو أن العالم كان يتغير على نحو أسرع كثيرا مما كان يمكن لأي شخص أن يتخيل. بحلول موعد مغادرة ستوديمان لـ «فورت ميد» في أبريل من العام 1992، كانت الحرب الباردة قد انتهت وحالفهم النصر فيها، وهي كانت الصراع الذي كان يبعث الحياة في وكالة الأمن القومي منذ نشأتها. الآن، حتى إن كانت الحاجة إلى إصلاح وكالة الأمن القومي مقبولة على نطاق واسع (وهي لم تكن كذلك)، فإن ذلك بدا على نحو مفاجئ أقل إلحاحا.

كان خلَف ستوديمان هو الأدميرال (اللواء البحري) مايك ماكونيل، الذي كان قد تولى إدارة مركز الاستخبارات المشتركة خلال عملية «عاصفة الصحراء». كان ماكونيل قد ظل ضابط الاستخبارات للجنرال باول خلال العام ونصف العام منذ الحرب. في منتصف الثمانينيات من القرن العشرين كان قد أمضى جولة عمل في مقر وكالة الأمن القومي استغرقت عاما، ملحقا بوحدة تعقب سلاح البحرية السوفييتية. لكن عودته إلى «فورت ميد» مديرا لوكالة الأمن القومي، في مثل تلك المرحلة من التحول الصارخ، لم تساعده على أن يعرف تماما ما الذي كان من المفترض أن يفعله هو وهذه الوكالة الضخمة.

كانت مديرية استخبارات الإشارة (سيجينت) بالوكالة تضم فرعين مستقلين: «المجموعة أ»، التي كانت ترصد وتراقب الاتحاد السوفييتي وأقماره الاصطناعية؛ و«المجموعة ب»، التي كانت ترصد وتراقب بقية العالم. وكما يشير اسمها كانت «المجموعة أ» هي فرع الصفوة، وكان جميع من في البناية يعرف ذلك. كان رعاياها يعيشون في أجواء نخبوية، كان هؤلاء هم الذين يحمون الأمة من القوة العظمى المناظرة؛ كانوا قد تعلموا مهارات متخصصة لا حصر لها، وكانوا قد غاصوا بعمق في العقلية السوفييتية، حتى إنهم كان باستطاعتهم الحصول على تيار من بيانات تبدو في ظاهرها عشوائية، ويستنبطون منها الأنماط وتغيراتها التي حينما تُجَمَّع أجزاؤها معا، كانت تقدم لهم (على الأقل نظريا) صورة عن نوايا الكرملين وتوقعات الحرب والسلام. أما الآن وقد انتهت الحرب الباردة فما النفع من تلك المهارات؟ هل كان مازال ينبغي أن يطلق على مراقبي الكرملين اسم المجموعة «أ»؟

كان لايزال الغموض الأكبر والأوسع نطاقا يتمثل في الكيفية التي كانت بها وكالة الأمن القومي ستواصل عملها في المراقبة والتنصت. بعد أسابيع من توليه منصبه مديرا، علم ماكونيل أن بعض أجهزة الاستقبال والهوائيات الراديوية (اللاسلكية)، التي كانت وكالة الأمن القومي قد وضعتها في جميع أنحاء العالم، لم تعد تلتقط إشارات. بدأت تتحقق «دراسة إمكانية الوصول العالمي (العمومي)» التي وضعها ستوديمان والتي تنبأت بالمعدل الذي كان سيتحول به العالم إلى الرقمية.

في الفترة ذاتها تقريبا دخل أحد معاوني ماكونيل إلى مكتبه حاملا معه خريطتين. كانت الخريطة الأولى هي خريطة العالم النمطية العادية، عليها أسهم

تحدد المسارات التي كانت قوى النقل البحري الرئيسية تبحر خلالها عبر المحيطات، وهي «خطوط الاتصال البحري» (sea lines of communication) أو «سلوكس» (SLOCs)، مثلما كان سيطلق عليها رجل من سلاح البحرية مثل ماكونيل. وكانت الخريطة الثانية تبين خطوط كابلات الألياف الضوئية وكثافاتها حول العالم.

قال معاونه وهو يشير إلى الخريطة الثانية «هذه هي الخريطة التي ينبغي لك أن تدرسها». كانت خطوط الألياف الضوئية هي «خطوط الاتصال البحري» (سلوكس) الجديدة، لكنها كانت مثل الثقوب الدودية(*) في المجرات، إذ إنها تنقلك في لمح البصر من نقطة ما إلى أخرى لحظيا.

فهم ماكونيل أوجه الشبه، والتلميح إلى التغيير، لكنه لم يدرك تماما تداعياته على مستقبل وكالته.

بعد فترة وجيزة من تلك الإحاطة شاهد ماكونيل فيلما جديدا باسم «المتسللون» (سنييكرز) Sneakers. كان إنتاجا بارعا، فيلما كوميديا مثيرا وذا مغزى، ويضم مجموعة من النجوم. كان السبب الوحيد وراء اهتمام ماكونيل بمشاهدة الفيلم هو أن أحد الأشخاص قد أخبره أن الفيلم عن وكالة الأمن القومي. كانت قصة الفيلم ساذجة، شركة صغيرة تضطلع بأعمال «القرصنة الحاسوبية الأخلاقية»(**) والتحري فائق التكنولوجيا، تُستأجر لسرقة صندوق أسود قابع على مكتب أحد العلماء الأجانب، يقول المستأجرون إنهم مع وكالة الأمن القومي

(*) من الناحية النظرية، «الثقوب الدودية» wormholes (تعرف أيضا باسم جسر آينشتاين-روزين Einstein–Rosen bridge) هي وصلات تخيلية تشبه النفق في الفضاء، وتوفر مسافة أقصر بين منطقتين منفصلتين في الكون. والفكرة هي أن مسافري الفضاء يمكن أن يستخدموا هذه الأنفاق لتجعل التنقل في الفضاء أقصر كثيرا من آلاف السنين، وتسمح للمسافر في أحدها بأن يخرج إلى كون آخر أو زمن آخر. ظهرت نظرية الثقوب الدودية لأول مرة في العام 1916، على يد الفيزيائي النمساوي لودفيغ فلام Ludwig Flamm، ولم يكن يطلق عليها هذا الاسم في ذلك الوقت. في العام 1935 استخدم ألبرت آينشتاين Albert Einstein والفيزيائي ناثان روزن Nathan Rosen نظرية النسبية العامة لتوضيح الفكرة، واقترحوا وجود «جسور» عبر الزمكان (دمج مفهومي الزمان والمكان) تربط نقطتين مختلفتين في الزمكان، مما يؤدي نظريا إلى إنشاء اختصار يمكن أن يقلل من وقت السفر والمسافة. [المترجم].

(**) «القرصنة الحاسوبية الأخلاقية» Ethical Hacking or white-hat hacking (يطلق عليها أحيانا «اختبار الاختراق» Penetration Testing) هي عملية تدخل أو اختراق منهجي لنظام أو شبكات الحاسوب يضطلع بها خبير في أمن المعلومات نيابة عن مالكي تلك الأنظمة وبإذن منهم، بهدف اكتشاف التهديدات أو نقاط الضعف التي ربما يجدها مهاجم خبيث ويستغلها، مما يسبب فقدان البيانات أو الخسارة المالية أو غيرها من الأضرار الكبرى. أما الغرض من القرصنة الحاسوبية الأخلاقية فإنه يتمثل في تحسين أمان الشبكة أو الأنظمة من خلال إصلاح الثغرات التي تُكتَشف في أثناء الاختبار. قد يستخدم القراصنة الأخلاقيون الأساليب والأدوات نفسها التي يستخدمها قراصنة الحاسوب (الهاكرز) الضارون. [المترجم].

وإن العالِم جاسوس. وكما اتضح الأمر، المستأجرون هم الجواسيس، والعالِم هو أحد مقاولي (متعهدي) الوكالة، والصندوق الأسود هو جهاز سري جدا يمكنه فك تشفير كل البيانات المشفرة، وترغب وكالة الأمن القومي في استعادته، وعمل التحري على القضية.

قرب نهاية الفيلم كان هناك مشهد يظهر فيه العبقري الشرير (أدى دوره بن كينغسلي Ben Kingsley)، وهو قرصان حاسوب (مخترق حاسوب) سابق مخادع، تبين أنه هو الذي طلب سرقة الصندوق الأسود، يتواجه مع المخبر الرئيسي (أدى دوره روبرت ريدفورد Robert Redford)، وهو صديقه القديم ورفيقه السابق من أيام عبثهما أثناء الدراسة الجامعية، وأفصح العبقري الشرير عن مناجاة قاتمة للنفس، موضحا سبب سرقته الصندوق.

في مقطع محموم تقول الشخصية التي يجسدها كينغسلي: «لم يعد العالم يُدار بالأسلحة، أو الطاقة، أو المال، إنه يُدار بالآحاد والأصفار، و«بتات» (أجزاء) ضئيلة من البيانات. إن كل شيء ما هو إلا إلكترونات... هنالك حرب حولنا، أيها الصديق القديم، حرب عالمية. إن الأمر لا يتعلق بمن لديه ذخيرة أكثر. الأمر يتعلق بمن يسيطر على المعلومات، ما نراه ونسمعه، وكيف نؤدي عملنا، وما الذي نفكر فيه. الأمر كله يتعلق بالمعلومات».

اعتدل ماكونيل في جلسته حينما شاهد[2] هذا المشهد. هنا، في هذا النموذج المستبعد لفيلم هوليوودي، كان بيان مهمة وكالة الأمن القومي الذي كان قد بحث عنه: ... العالم يُدار بالآحاد والأصفار.. هنالك حرب حولنا... الأمر يتعلق بمن يسيطر على المعلومات.

حينما عاد ماكونيل إلى «فورت ميد»، أخبر الجميع عن فيلم «المتسللون»، وشجع كل موظف تحت إدارته على الذهاب لمشاهدته. إنه حتى حصل على بكرة النسخة النهائية للفيلم، وعرضها على شاشة ليشاهده كبار مسؤولي الوكالة، مخبرا إياهم أن هذه هي رؤية المستقبل التي يجب عليهم أن يضعوها نصب أعينهم وفي صدارة اهتماماتهم.

في ذلك الوقت لم يكن ماكونيل يعرف أن سيناريو فيلم «المتسللون» كان قد كتبه لاري لاسكر ووالتر باركس، الثنائي الذي كان قد كتب «ألعاب الحرب (المناورات

الحربية)» قبل عقد من الزمان. كان فيلم «المتسللون» أيضا سيُحدث تأثيرا في السياسة القومية، على رغم أنه ليس بالقدر نفسه.

فور إدراكه الحقيقة المستوحاة من الفيلم استدعى ماكونيل ريتشارد ويلهلم، الذي كان مفوض وكالة الأمن القومي، هو في الواقع كان ساعد ماكونيل الأيمن في مركز الاستخبارات المشتركة في أثناء «عاصفة الصحراء». بعد الحرب، كان ويلهلم وريتشارد هافر قد كتبا تقريرا لخصا فيه أنشطة المركز، وسردا الدروس المستفادة للأخذ بها في عمليات استخبارات الإشارة (سيجينت) المستقبلية. على سبيل المكافأة عُجِّلت ترقية ويلهلم ليتولى قيادة محطة التنصت التابعة لوكالة الأمن القومي في قاعدة «ميساوا» Misawa الجوية في اليابان، وهي واحدة من أكبر مواقع الوكالة الخارجية. كان ويلهلم متربعا على قمة ترتيب ضباط وكالة الأمن القومي الميدانيين.

لكن الآن طلب ماكونيل من ويلهلم العودة إلى «فورت ميد»، وأن يتولى وظيفة جديدة أنشأها خصيصا من أجله. سيكون مسماها هو «مدير وسائل حرب المعلومات». (هنالك حرب حولنا... الأمر يتعلق بمن يسيطر على المعلومات).

انتشر المفهوم والمصطلح. في شهر مارس التالي أصدر الجنرال كولن باول، رئيس الهيئة المشتركة لرؤساء الأركان، مذكرة سياسات بشأن «وسائل حرب المعلومات»، التي عرفها على أنها عمليات «فصل رأس هيكل قيادة العدو عن جسده من القوات المقاتلة»[3]. استجابت كل فروع القوات المسلحة في الوقت نفسه تقريبا، وأُنشئ مركز سلاح الجو لوسائل حرب المعلومات، ونشاط وسائل حرب المعلومات البحرية، ونشاط وسائل حرب المعلومات البرية بالجيش الميداني (القوات البرية). (كانت هذه الكيانات موجودة بالفعل، ولكنها كانت تحت أسماء مختلفة).

بحلول الوقت الذي شاهد فيه ماكونيل فيلم «المتسللون» Sheakers، كان قد أُطلِع بشكل كامل على برامج سلاح البحرية ووكالة الأمن القومي لوسائل الحرب المضادة للقيادة والسيطرة، وكان مفتونا بإمكانات تطبيق المفهوم على العصر الجديد. كانت «وسائل حرب المعلومات» هي في الأساس وسائل الحرب المضادة للقيادة والسيطرة مضافة إليها التكنولوجيا الرقمية. وفي تجسيدها العصري الحديث كان بإمكان ماكونيل أن يقلب استخبارات الإشارة (سيجينت) رأسا على عقب، لم يعد الأمر اعتراض إشارة فقط، بل النفاذ إلى مصدرها، وحالما يولَج إلى السفينة الأم،

نظام القيادة والسيطرة الخاص بالعدو، كان يمكن تغذية النظام بمعلومات خاطئة كاذبة، أو تغيير، أو عرقلة، أو تدمير الآلة، وإرباك القادة. السيطرة على المعلومات للحفاظ على السلام وكسب الحرب.

لم يأتِ شيء من هذا إلى ويلهلم في صورة مادة إخبارية، لقد كان طوال أعوام يناوش على خطوط جبهة حرب المعلومات. لكن بعد ستة أسابيع من توليه منصبه الجديد، جاء إلى مكتب ماكونيل وقال: «مايك، يجري العبث معنا هنا نوعا ما».

كان ويلهلم قد غاص في التفاصيل بشأن شكل حرب المعلومات والكيفية التي يمكن أن تبدو بها تلك الحرب ثنائية الاتجاه، التي يستخدم كلا طرفيها الأسلحة ذاتها، ولم يكن المشهد جيدا. كانت الثورة في الإشارات الرقمية والإلكترونيات الدقيقة تتغلغل في الجيش الأمريكي والمجتمع الأمريكي بذريعة الكفاءة. كان الجنرالات والرؤساء التنفيذيون للشركات على حد سواء يربطون كل شيء بشبكات الحاسوب. كان اعتماد الولايات المتحدة على هذه الشبكات آخذا في النمو أكثر من أي دولة على وجه الأرض، وما يقرب من 90 في المائة من الملفات الحكومية - بما في ذلك ملفات الاستخبارات - كانت تتدفق جنبا إلى جنب مع البيانات التجارية. صار التحكم في البنوك (المصارف)، وشبكات الكهرباء، وخطوط الأنابيب، ونظام نداء الطوارئ 911، يحدث كله من خلال الشبكات، التي كانت جميعها غير حصينة وعرضة للهجوم، وعرضة لأبسط أنواع القرصنة (الاختراق).

حينما فكر ويلهلم في مهاجمة شبكات الآخرين أخبر ماكونيل، ضع في اعتبارك أنهم يمكنهم أن يفعلوا بنا الأشياء نفسها. لم تكن وسائل حرب المعلومات تتعلق باكتساب أفضلية في المعركة، بل كان ينبغي أيضا أن تتناول حماية الأمة من جهود الدول الأخرى للحصول على الأفضلية نفسها.

كان ذلك إعادة اكتشاف لتحذير ويليس وير الذي أطلقه قبل ذلك بربع قرن.

على الفور، استوعب ماكونيل أهمية رسالة ويلهلم. لم يكن مركز أمن الحاسوب، الذي أنشأه بوبي راي إنمان قبل عقد من الزمان، قد جذب إلا القليل من التمويل أو الاهتمام. أما مديرية أمن المعلومات (التي تسمى الآن مديرية ضمان المعلومات) فهي مع ذلك - حرفيا - شيء ثانوي، وكانت على بعد عشرين دقيقة بالسيارة من المقر الرئيسي.

في هذه الأثناء كان إرث التوجيه الرئاسي بشأن أمن الحاسوب (إن إس دي دي - 145) الذي أصدره ريغان، يرقد في حالة يرثى لها. ما نفّذه عضو الكونغرس جاك بروكس Jack Brooks من إصلاح شامل للتوجيه، ونص عليه قانون أمن الحاسوب في العام 1987، كان قد أعطى وكالة الأمن القومي الهيمنة على أمن الحواسيب العسكرية والشبكات المصنفة على أنها سرية، لكنه وجه المكتب القومي للمعايير (للتوحيد القياسي) التابع لوزارة التجارة، للتعامل مع بقية الأمور. كانت المعادلة محكوما عليها بالفشل منذ البداية. كان المكتب القومي للمعايير (للتوحيد القياسي) يفتقر إلى الكفاءة التقنية، في حين كانت وكالة الأمن القومي تفتقر إلى الرغبة المؤسسية. حينما كان يكتشف أحد في مديرية ضمان المعلومات أو في مركز أمن الحاسوب وجود خلل أو ثغرة أمنية في إحدى برمجيات الحاسوب التي ربما تستخدمها دولة أخرى، فإن السلطة الحقيقية في وكالة الأمن القومي - المحللين في مديرية استخبارات الإشارة (سيجينت) – كانت ترغب في استغلالها وليس إصلاحها، كانوا يرون أنها سبيل جديد للنفاذ إلى شبكة دولة أجنبية واعتراض اتصالاتها.

بعبارة أخرى لم يتعد الأمر أكثر من تجاهل المشكلة؛ بالأحرى، لم يكن أحد في السلطة يرى الأمر على أنه مشكلة.

عزم ماكونيل على تغيير ذلك. ارتقى بمديرية ضمان المعلومات، ومنحها مزيدا من المال في حين كانت الموازنة العامة الإجمالية تُخفض، لم يقتصر الأمر على وكالة الأمن القومي ولكنه شمل وزارة الدفاع بأسرها. بدأ ماكونيل في تحريك الأفراد جيئة وذهابا، بين مديرية استخبارات الإشارة (سيجينت) ومديرية ضمان المعلومات، لتنفيذ مهام قصيرة الأجل فقط، لكن الفكرة كانت التقاء الثقافتين إحداهما بالأخرى.

لم يكن هذا أكثر من بداية. كان لدى ماكونيل الكثير على كاهله، خفض الموازنة، والتحول المتسارع من الدوائر التماثلية (التناظرية) إلى الحزم الرقمية، والانخفاض الحاد في الإشارات الراديوية (اللاسلكية)، وما ينتج عن ذلك من حاجة إلى إيجاد وسائل جديدة لاعتراض الاتصالات. (بعد فترة وجيزة من تنصيب ماكونيل مديرا، وجد نفسه مضطرا إلى إيقاف تشغيل أحد هوائيات وكالة الأمن القومي في آسيا لأنه لم يعد يلتقط أي إشارات راديوية (لاسلكية). إن كل حركة البيانات التي كانت

في ذروتها يجري يوميا رصدها بحجم هائل، قد حُوِّلت إلى كابلات تحت الأرض أو إلى الفضاء السيبراني).

في خريف العام 1994 شاهد ماكونيل في مكتبه بيانا عمليا لبرمجية «نتسكيب ماتريكس» Netscape Matrix، أحد أوائل المتصفحات (المستعرضات) التجارية لشبكة الحاسوب، وجال بخاطره أن «هذا سيغير العالم». صار لدى كل شخص إمكانية الوصول إلى شبكة الإنترنت، لم يقتصر الأمر على الحكومات الحليفة والمنافسة، بل الأفراد، بمن في ذلك الإرهابيون. (كان التفجير الأول لمركز التجارة العالمي قد حدث في العام الذي سبق؛ الإرهاب - الذي كان ينظر إليه على أنه مصدر إزعاج أثناء سباق التسلح النووي والحرب الباردة - كان آخذا في الظهور كتهديد رئيسي). مع نهوض الإنترنت ظهر التشفير بصفة تجارية، للحفاظ على اتصالات الشبكة آمنة إلى حد ما. لم يعد إعداد الشفرات حكرا على وكالة الأمن القومي وما يناظرها، كان الجميع يفعل ذلك، بما في ذلك الشركات الخاصة في «وادي السيليكون» وعلى طول الطريق 128 بالقرب من «بوسطن»(*)، والتي كانت تقارب البراعة التقنية للوكالة. خشي ماكونيل أن تفقد وكالة الأمن القومي بريقها الفريد المتمثل في قدرتها على الولوج إلى، والتنصت على، الاتصالات التي تؤثر في الأمن القومي.

أصبح ماكونيل يدرك أيضا أن الوكالة لم تكن مجهزة لاغتنام التغييرات المقبلة. كان الشاب كريستوفر ميلون Christopher Mellon، أحد موظفي لجنة مجلس الشيوخ المعنية بالاستخبارات، يداوم على أن يأتي كثيرا إلى الوكالة طارحا أسئلة. كان ميلون قد استمع إلى جلسات الإحاطة بشأن عمليات تكيف «فورت ميد» مع العالم

(*) يرجع تاريخ الطريق 128 إلى عشرينيات القرن العشرين، حينما سعت وزارة الأشغال العامة بولاية بوسطن إلى تخفيف الازدحام المروري الناتج عن سرعة تزايد عدد السيارات والشاحنات في شوارع بوسطن، وأُنشئ طريق محيطي (دائري). لكن، سرعان ما اتضح أن القيادة عبر الطريق المحيطي (الدائري) كانت بطيئة، فبدأت الولاية التخطيط لطريق سريع حديث يوفر للسائقين وسيلة للتحايل على حركة المرور في بوسطن. في العام 1951 افتُتِح الجزء الأول من الطريق 128، وبحلول العام 1956 امتد الطريق السريع مسافة 65 ميلا من مدينة «غلوستر» Gloucester إلى مدينة «برينتري» Braintree. وبينما كان المسؤولون واثقين بأن الطريق سيخفف حركة المرور في بوسطن ويساعد على تسهيل السفر بين الضواحي المتنامية في المنطقة، فإنهم لم يتوقعوا أن يصبح الطريق 128 في حد ذاته وجهة ومحركا اقتصاديا. لكن المطورين العقاريين جاءوا بابتكاراتهم الخاصة - أول المجمعات الصناعية الحديثة - التي كانت مواقع مثالية لعدد متزايد من شركات التكنولوجيا في الولاية. أدت متاخمة المنطقة لمختبرات الجامعة وتوسع مجتمعات الضواحي إلى جذب الكثير من شركات التكنولوجيا المتقدمة إلى المنطقة التي أطلق عليها اسم الطريق 128، والتي تطورت سريعا لتكون أول «ممر للتكنولوجيا المتقدمة» في البلاد. [المترجم].

الرقمي الجديد، لكنه حينما حضر إلى المقر وفحص السجلات، اكتشف أن موازنة الوكالة التي تبلغ 4 مليارات دولار، منها مليونا دولار فقط هي المخصصة لبرامج اختراق الاتصالات على الإنترنت. طلب ميلون أن يرى الأفراد المكلفين بهذا البرنامج. وجرى اصطحابه إلى ركن بعيد منزوٍ من الطابق الرئيسي، حيث كان هناك بضع عشرات من التقنيين - من بين قوة العمل التي تقدر بعشرات الآلاف - يعبثون بأجهزة الحاسوب.

لم يكن ماكونيل قد عرف مدى ضآلة هذه الجهود، وأكد للجنة مجلس الشيوخ أنه كان سيضع أمر تعزيز البرامج على رأس الأولويات. لكنه انشغل بما اعتبره مشكلة أكثر إلحاحا، ظهور التشفير الصوتي بصفة تجارية، والذي كان قريبا سيجعل من الصعب على وكالة الأمن القومي (ومكتب التحقيقات الفدرالي) التنصت على المحادثات الهاتفية. ابتكر طاقم عمل ماكونيل ما اعتبروه حلا للمشكلة، «رقاقة كليبر» (Clipper Chip)، وهي مفتاح تشفير وصفوه بأنه آمن تماما، وكانت الفكرة هي تنصيب الرقاقة في كل جهاز اتصالات. كانت الحكومة ستتمكن من الولوج إلى المحادثات الهاتفية والتنصت عليها، فقط إذا اتبعت إجراء مطولا يتكون من شقين (مفتاحين). كان سيتعين على أحد العملاء الذهاب إلى «المعهد القومي للمعايير والتكنولوجيا» (National Institute of Standards and Technology)، الذي يسمى حاليا «المكتب القومي للمعايير» (National Bureau of Standards)، من أجل الحصول على أحد مفتاحي التشفير محفوظا على قرص مرن. عميل آخر كان سيذهب إلى وزارة الخزانة للحصول على المفتاح الآخر؛ ثم يذهب العميلان إلى القاعدة البحرية في «كوانتيكو» Quantico بولاية فيرجينيا Virginia، لإدخال كلا القرصين في حاسوبٍ سيفكُّ التشفير.

جاهد ماكونيل بقوة من أجل «رقاقة كليبر»[4] وجعلها في صدارة أولوياته، لكنها كانت محكوما عليها بالفشل منذ البداية. أولا، كانت باهظة الثمن، إذ إن الهاتف المزود برقاقة كليبر كان سيكلف أكثر من ألف دولار. ثانيا، كان الإجراء ذو المفتاحين غريبا وشديد التكلف. (شاركت دوروثي دينينغ Dorothy Denning، وهي من أفضل علماء التشفير في البلاد، في تدريب محاكاة، حصلت على المفتاح من وزارة الخزانة؛ لكن، وهي في طريقها إلى «كوانتيكو»، علمت أن الشخص الذي ذهب إلى

«المعهد القومي للمعايير والتكنولوجيا» كان قد أخذ المفتاح الخطأ، ولم يتمكنوا من فك التشفير). أخيرا، كانت هناك العقبة الكبرى، كان عدد قليل جدا من الأشخاص يثق بـ «رقاقة كليبر»، لأن عددا قليلا جدا من الناس كان يثق بدوائر الاستخبارات. كانت لاتزال حاضرة في الأذهان تلك المكاشفات التي أطلقتها لجنة السيناتور فرانك تشيرتش Frank Church في منتصف السبعينيات من القرن العشرين بشأن اضطلاع وكالة الاستخبارات المركزية ووكالة الأمن القومي بالمراقبة المحلية. كان الجميع تقريبا - حتى أولئك الذين لم يكونوا يميلون إلى عدم الثقة بدوائر التجسس - يشتبهون في أن وكالة الأمن القومي قد برمجت «رقاقة كليبر» بباب خلفي سري كان عملاؤها يستطيعون فتحه، ومن ثم يستمعون إلى المحادثات الهاتفية، من دون المرور بوزارة الخزانة، أو المعهد القومي للمعايير والتكنولوجيا، أو أي إجراء قانوني.

انتهى أمر «رقاقة كليبر» مع تذمر وأنين. وكانت محاولة من ماكونيل للتوصل إلى حل وسط بين الخصوصية الشخصية والأمن القومي، وتنفيذ ذلك علانية، أمام أعين العامة. إنها كانت محاولة حسنة النيات، لكنها كانت غير صائبة. المرة التالية، حينما تنشئ أو تكتشف وكالة الأمن القومي أبوابا خلفية إلى البيانات، كانت ستفعل ذلك مثلما كانت تفعل دائما، تحت عباءة من السرية.

3

«بيرل هاربر» سيبرانية

«يمكن لهجوم منسق ينفذه حفنة من الخبراء التقنيين المحترفين - من نهاية الشارع فقط أو من الجانب الآخر من الكرة الأرضية - أن يدمر الأمة ويعصف بها»

في 19 أبريل 1995 عمدت عصبة صغيرة من الأناركيين(*) (اللاسلطويين) المتشددين، يتزعمها تيموثي ماكفي Timothy McVeigh، إلى تفجير بناية مكاتب فدرالية في مدينة أوكلاهوما سيتي Oklahoma City، مما أسفر عن مقتل 168

(*) أناركي: كلمة يونانية قديمة تعني حرفيا لا حاكم أو لا سلطة، وقد استُخدمت الكلمة طوال قرون في الكتابات الغربية لتشير إلى حالة بلد أو إقليم جغرافي حال تفكك أو سقوط السلطة المركزية المسيطرة عليه مما يؤدي إلى صعود قوى مختلفة تتصارع على أن تحل محلها محدثة حالة من فوضى الحرب الأهلية، ثم أصبحت الكلمة في اللغات الأوروبية المختلفة مرادفا للفوضى. في المقابل، فإن الأناركية بوصفها نظرية وفكرا سياسيا، وباعتبارها حركة اجتماعية تبلورت لأول مرة في النصف الثاني من القرن التاسع عشر في إطار نشأة الحركات العمالية والاشتراكية، واتخذ بعض أوائل مفكريها اسم الأناركية بمعنى اللاسلطوية، إذ دعوا إلى أن ينظم المجتمع شؤونه ذاتيا من دون تسلط لفرد أو جماعة على مقدرات وحياة غيرهم. تعني اللاسلطوية الغياب التام للسلطة وليس تفكيك السلطة المركزية إلى سلطات متناحرة تحدث الفوضى في المجتمع، وهي تعني استبدال مؤسسات الدولة المركزية والهرمية بمؤسسات شعبية أفقية - أي لا تكون فيه تراتبية هرمية - وشبكية - أي لا مركزية ترتبط كل منها بالأخرى للتكامل ولإدارة الموارد المشتركة واتخاذ القرار فيما يخصها. [المترجم].

شخصا، بالإضافة إلى إصابة 600 شخص، وتدمير أو إلحاق الضرر بنحو 325 بناية في دائرة نصف قطرها ستة عشر بلوكًا (مجموعة بنايات)، مما سبب خسائر تقدر بأكثر من 600 مليون دولار. والأمر الصادم الذي تمخض عنه التحقيق اللاحق هو مدى سهولة نجاح ماكفي ومشاركيه في تنفيذ هذا التفجير. لم يتطلب الأمر أكثر من شاحنة وبضع عشرات من أكياس نترات الأمونيوم، وهي مادة كيميائية شائعة في الأسمدة الزراعية، ويمكن الحصول عليها من الكثير من متاجر لوازم الزراعة. عمليا كان الأمن حول البناية غير موجود.

كان السؤال البديهي الجلي، داخل الحكومة وخارجها، هو عن أنواع الأهداف التي كانت ستُفجَّر لاحقا، هل هي أحد السدود، أو ميناء رئيسي، أو الاحتياطي الفدرالي، أو محطة للطاقة النووية؟ إن ضرر أي من تلك الضربات كان سيفوق القول إنه مجرد حادث مأساوي مفجع، إنه ضرر يمكن أن يكون له دوي وأصداء عبر الاقتصاد برمته. إذن، إلى أي مدى كانت تلك الأهداف غير حصينة وعرضة للخطر، وما الذي كان يمكن فعله لحمايتها؟

في 21 يونيو وقَّع بيل كلينتون على قرار توجيه رئاسي «بي دي دي - 39» PDD-39، بعنوان «سياسة الولايات المتحدة بشأن مكافحة الإرهاب»، وهو توجيه وضع - من بين أمور أخرى - المدعية العامة جانيت رينو Janet Reno مسؤولة عن «لجنة مجلس الوزراء» لفحص ومراجعة، واقتراح طرق لتقليص، أوجه ضعف «المرافق الحكومية» و«البنية الأساسية القومية الحرجة البالغة الأهمية»[1] وقابليتها للتعرض للخطر.

حولت رينو المهمة[2] إلى نائبتها جايمي غوريليك Jamie Gorelick، التي بدورها شكلت مجموعة عمل للبنية الأساسية الحرجة البالغة الأهمية، تتألف من مفوضين آخرين من البنتاغون، ووكالة الاستخبارات المركزية، ومكتب التحقيقات الفدرالي، والبيت الأبيض. بعد بضعة أسابيع من الاجتماعات أوصت المجموعة بأن يسمي الرئيس لجنة، عقدت بدورها جلسات استماع، وكتبت تقريرا أسفر عن صياغة مسودة توجيه رئاسي آخر.

فوجئ العديد من هيئة موظفي البيت الأبيض، الذين حسبوا أن اللجنة كانت ستخرج بوسائل جديدة لتأمين المنشآت المادية المهمة، إذ إن أكثر من نصف تقريرها

وتوصياتها تناول أوجه الضعف والثغرات الأمنية لشبكات الحاسوب والحاجة الملحة لما أسمته اللجنة «الأمن السيبراني».

نشأ ذلك التحول المفاجئ من أن الأعضاء الرئيسيين في مجموعة عمل البنية الأساسية الحرجة، وفي اللجنة الرئاسية اللاحقة، كانوا قد جاءوا من وكالة الأمن القومي، أو من البرامج السوداء فائقة السرية بسلاح البحرية، ومن ثم كانوا على دراية كاملة بهذا الجانب الجديد من العالم.

كان ريتشارد ويلهلم، مدير وسائل حرب المعلومات في وكالة الأمن القومي، من بين الأعضاء الأكثر تأثيرا في مجموعة العمل. قبل بضعة أشهر من التفجير الذي وقع في مدينة أوكلاهوما سيتي كان الرئيس كلينتون قد عين نائبه آل غور Al Gore مسؤولا عن الإشراف على مشروع «رقاقة كليبر»، وأوفد مايك ماكونيل ويلهلم إلى البيت الأبيض بوصفه مفوض وكالة الأمن القومي بشأن المشروع، وسرعان ما ماتت الرقاقة، لكن غور استبقى ويلهلم وعينه مستشارا له لشؤون الاستخبارات، مع منصب في هيئة مجلس الأمن القومي. في بدايات وظيفته الجديدة أخبر ويلهلم بعض زملائه الموظفين بشأن الاكتشافات التي حققها في «فورت ميد»، وخصوصا تلك التي تسلط الضوء على أوجه الضعف والثغرات الأمنية للمجتمع الأمريكي الذي يتزايد ترابطه الشبكي الحاسوبي. كتب ويلهلم مذكرة حول هذا الموضوع إلى مستشار كلينتون للأمن القومي، أنتوني ليك Anthony Lake، الذي بدوره وقعها باسمه الخاص ورفعها إلى الرئيس.

عندما شكلت جايمي غوريليك فريق العمل الخاص بها كان من الطبيعي أن يكون ويلهلم من بين أعضاء الفريق. كانت إحدى أولى مهام اللجنة هي تعريف مسماها، واستجلاء ماهية البنيات الأساسية الحرجة، وتحديد أي القطاعات كان حيويا وضروريا للمجتمع الحديث. خلصت المجموعة إلى قائمة تضم ثمانية قطاعات، هي: الاتصالات، والطاقة الكهربائية، والغاز والنفط، والخدمات المصرفية والمالية، والنقل، وإمدادات المياه، وخدمات الطوارئ، و«استمرارية الحكومة» في حالة وقوع حرب أو كارثة.

أشار ويلهلم إلى أن جميع هذه القطاعات تعتمد على شبكات الحاسوب، واعتمادا كبيرا في بعض الحالات. لن يكون الإرهابيون في حاجة إلى تفجير بنك، أو

خط سكة حديد، أو شبكة كهرباء، كان يمكنهم الاكتفاء بتعطيل شبكة الحاسوب التي تتحكم في تشغيلها، ولن تختلف النتيجة. نتيجة ذلك دفعَ ويلهلم بأن «البنية الأساسية الحرجة» ينبغي ألا تشتمل على البنى المادية فقط، بل أيضا التجهيزات لما كان سيطلق عليه قريبا الفضاء السيبراني.

لم تكن غوريليك في حاجة إلى إقناع بشأن هذه النقطة، فهي بوصفها نائبة للمدعية العامة، كانت قد عملت في عدة لجان مشتركة بين الوكالات، وتناولت إحدى هذه اللجان مسائل متعلقة بالأمن القومي. تشاركت غوريليك رئاسة هذه اللجنة مع نائب مدير وكالة الاستخبارات المركزية، الذي تصادف أنه كان بيل ستوديمان، المدير السابق لوكالة الأمن القومي (وأحد تلاميذ بوبي راي إنمان). لقد كان ستوديمان في أيام وجوده في «فورت ميد» مدافعا حادا عن وسائل الحرب المضادة للقيادة والسيطرة، المعروفة الآن باسم وسائل حرب المعلومات، متضمنة كلا جانبيها الهجومي والدفاعي، أي قدرة أمريكا على أن تنفذ إلى شبكات العدو، وقدرة العدو على أن ينفذ إلى شبكات أمريكا. وفي لانجلي كان ستوديمان يروج للفكرة ذاتها.

كان ستوديمان يتقابل مع غوريليك كل أسبوعين لمناقشة هذه القضايا، وقد كان لحججه ودفوعه صداها. قبل تعيين غوريليك نائبا للمدعية العامة كانت قد عملت محامية عامة في البنتاغون، حيث استمعت إلى إحاطات عديدة حول ما حدث من اختراق لمقاولي (متعهدي) وزارة الدفاع، وحتى لوزارة الدفاع ذاتها. وفي وزارة العدل كانت غوريليك تساعد على الملاحقة القضائية الجنائية للمتسللين الذين قد نفذوا إلى حواسيب البنوك والمصنعين. قبل عام من حادثة مدينة أوكلاهوما سيتي كانت غوريليك قد ساعدت على صياغة مسودة خطة عمل مبادرة الجريمة الحاسوبية، التي كانت تهدف إلى تعزيز خبرة وزارة العدل في «مسائل التكنولوجيا الفائقة»[3]، كما ساعدت على إنشاء لجنة تنسيق فريق مهمة البنية الأساسية المعلوماتية.

لم تكن تلك المغامرات مجرد موضوعات تستهويها، بل كانت قد صدر بها تكليف رسمي، وكانت تعد ضمن عبء قضايا وزارة العدل. في الآونة الأخيرة[4] كانت منظمة إجرامية روسية قد اخترقت حواسيب بنك «سيتي بنك» Citibank وسرقت 10 ملايين دولار، وحولتها إلى حسابات منفصلة في كاليفورنيا،

وألمانيا، وفنلندا، وإسرائيل. كان أحد الموظفين السابقين في شبكة إنذار حالات الطوارئ، التي تغطي 22 دولة، ساخطا، فاقتحم النظام وأسقطه مدة عشر ساعات. وسيطر أحد الأشخاص في ولاية كاليفورنيا على الحاسوب الذي يدير شبكة مبدلات الهاتف المحلية، وحمّل معلومات بشأن تنصُّت الحكومة على الإرهابيين المشتبه فيهم، ونشر المعلومات على الإنترنت. عمد صبيّان مراهقان، قرينان شريران لبطل فيلم «ألعاب الحرب (المناورات الحربية)»، إلى اختراق شبكة حاسوب قاعدة للقوات الجوية في مدينة رومي Rome بولاية نيويورك. في وقت لاحق سخر أحد الصبية من أن المواقع العسكرية كانت هي الأسهل اختراقا على مستوى الإنترنت بأسرها.

بناء على كل هذا، خبراتها بوصفها محامية الحكومة، والاجتماعات المشتركة بين الوكالات مع ستوديمان[5]، ومن خلال المناقشات الحالية مع ريتشارد ويلهلم في مجموعة العمل، توصلت غوريليك إلى استنتاجين مثيرين للقلق. أولا، على الأقل في هذا المضمار، كانت التهديدات من المجرمين، والإرهابيين، والخصوم الأجانب جميعها متشابهة، كانوا جميعا يستخدمون وسائل الهجوم ذاتها؛ التي في كثير من الأحيان، لم يكن من الممكن تمييزها. لم تكن تلك المشكلة تخص فقط وزارة العدل أو وزارة الدفاع، كان يتعين على الحكومة بكاملها أن تتعامل مع المشكلة، ولأن معظم حركة بيانات الحاسوب تمر عبر شبكات مملوكة لشركات خاصة، كان ينبغي أن يساعد القطاع الخاص أيضا على إيجاد الحلول وإنفاذها.

ثانيا، كان التهديد أوسع وأعمق مما كانت غوريليك قد تخيلت. حينما فحصت قائمة البنى الأساسية الحرجة التي أعدتها مجموعة العمل، ونظرا إلى تزايد التحكم في تلك البنى بواسطة الحواسيب، أدركت غوريليك في لحظة ذهول، أن هجوما منسقا ينفذه حفنة من الخبراء التقنيين المحترفين، من نهاية الشارع فقط أو من الجانب الآخر من الكرة الأرضية، يمكن أن يدمر الأمة ويعصف بها.

عضد هذا الفهم الجديد إحاطة قدّمها مفوض البنتاغون في مجموعة العمل، وهو ضابط متقاعد من سلاح البحرية يدعى برينتون غرين Brenton Greene، كان قد عُيِّن أخيرا في منصب جديد هو مدير سياسات البنية الأساسية، في مكتب الأمن العام لوزارة الدفاع.

كان غرين قد شارك في بعض البرامج العسكرية الأكثر سرية. في أواخر الثمانينيات وأوائل التسعينيات من القرن العشرين، كان قائدا لإحدى الغواصات في مهمة تجسس فائقة السرية. بعد ذلك أدار برامج البنتاغون السوداء (السرية) في وحدة كانت تسمى «القسم جيه» (J Department)، الذي كان يعمل على تطوير واستحداث تكنولوجيات ناشئة قد تمنح أمريكا أفضلية في حرب آتية. كان أحد أفرع «القسم جيه»[6] يعمل على «استهداف العقدة الحرجة». كانت الفكرة هي تحليل البنى الأساسية لكل بلد خصم وتحديد الأهداف الرئيسية، أقل عدد من الأهداف التي كان سينبغي للجيش الأمريكي تدميرها من أجل إحداث تأثير كبير على مسار الحرب. ساعد غرين على استحداث فرع آخر في القسم، وهو مشروع «التعزيز الاستراتيجي»، الذي ركز على سبل جديدة للنفاذ إلى شبكات القيادة والسيطرة الخاصة بالخصوم الأجانب وتقويضها، وهذا هو جوهر وسائل حرب المعلومات.

من خلال العمل على تلك المشروعات، ورؤية أنه - على الأقل من الناحية النظرية - كم كان من السهل تدمير بلد أجنبي ببضع قنابل تُزرع على نحو مدروس بعناية، أو بعمليات اقتحام إلكترونية. ومثلما كان العديد ممن سلكوا هذا الطريق من قبله قد أدركوا، أدرك غرين الجانب الآخر من المعادلة: ما كان باستطاعتنا أن نفعل بهم، كان باستطاعتهم فعله بنا. وكان غرين يعرف أيضا أن أمريكا عرضة لتلك الأنواع من الهجمات، لا سيما الهجمات المعلوماتية، أكثر من أي دولة أخرى على هذا الكوكب.

في معرض بحثه صادف غرين دراسة بعنوان «قابلية التأثر المادي للأنظمة الكهربائية من الكوارث الطبيعية والتخريب» Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage، كان مكتب الولايات المتحدة لتقييم التكنولوجيا - وهو مجموعة استشارية تتبع الكونغرس - قد أجراها في العام 1990. في الصفحات الافتتاحية من الدراسة كشف معدوها عن محطات الطاقة والمحولات الكهربائية التي إذا عُطِّلت كانت ستسقط وتعطل مجموعة هائلة من خطوط الشبكة القومية. كانت هذه الوثيقة عامة وعلنية، ومتاحة لأي شخص كان يعرف عنها.

علم غرين من أحد زملائه في «القسم جيه» أنه بعد فترة وجيزة من دخول جورج بوش George Bush إلى البيت الأبيض في يناير من العام 1989، عرض

السيناتور (عضو مجلس الشيوخ) جون جلين John Glenn الدراسة على الجنرال برنت سكوكروفت Brent Scowcroft، مستشار بوش للأمن القومي. ساور سكوكروفت بعض القلق، وطلب من ضابط في الخدمة السرية يدعى تشارلز لين Charles Lane تشكيل فريق عمل مصغر لا يزيد على ستة أفراد من المحللين التقنيين لإجراء دراسة منفصلة. كانت النتائج التي توصل إليها الفريق مزعجة جدا، إلى درجة أن سكوكروفت مزّق كل مواد العمل الخاصة بالفريق، وطُبعت نسختان فقط من تقرير لين. حصل غرين على واحدة منهما.

عند هذه النقطة استنتج غرين أنه كان يعمل على الجانب الخطأ من المسألة، إن حماية البنية الأساسية لأمريكا كانت أكثر أهمية - وكما رآها، أكثر إلحاحا - من البحث عن سبل لإحداث ثغرات في البنى الأساسية الأجنبية.

كان غرين يعرف لينتون ويلز Linton Wells، وهو ضابط زميل له في سلاح البحرية الأمريكية لديه خلفية عميقة في البرامج السوداء (السرية)، وكان حينذاك مساعدا عسكريا لوالتر سلوكومب Walter Slocombe، وكيل وزارة الدفاع لشؤون السياسة. أخبر غرين ويلز أن سلوكومب كان ينبغي أن يستعين بمدير لسياسة البنية الأساسية. وافق سلوكومب على الفكرة، وعُيِّن غرين.

في أثناء الأشهر القليلة الأولى التي قضاها غرين في الوظيفة الجديدة، عمل على تقديم بيان حول «الترابط والاعتماد المتبادل» فيما بين البنية الأساسية للبلاد، وتركزها، واختلاط قطاعاتها بعضها مع بعض، والكيفية التي يمكن بها لعرقلة بعض «العقد الحرجة» (عبارة مأخوذة من القسم جيه) أن تلحق بالبلاد أضرارا جسيمة.

على سبيل المثال عرف غرين أن «مؤسسة بيل» Bell Corporation وزعت قرصا مدمجا يحتوي على قائمة بكل مبدلات الاتصالات الخاصة بها في جميع أنحاء العالم، وذلك حتى يتسنى لشركة هاتف في الأرجنتين، على سبيل المثال، أن تعرف كيفية توصيل الدوائر لتوجيه مكالمة هاتفية إلى أوهايو Ohio. نظر غرين إلى تلك القائمة وفي ذهنه سؤال مختلف: أين جميع مبدلات الاتصالات في المدن الأمريكية الكبرى؟ في كل حالة فحصها، ولأسباب تتعلق بالجدوى الاقتصادية، كانت مبدلات الاتصالات تتركز في موقعين فقط. بالنسبة إلى مدينة نيويورك New York كان معظم مبدلات الاتصالات يقع في عنوانين في مانهاتن السفلى (جنوب مانهاتن)؛

هما: 140 ويست ستريت West Street و104 برود ستريت Broad Street. إذن، تخلص من هذين العنوانين، سواء بقنبلة أو بهجوم بوسائل حرب المعلومات، وكانت مدينة نيويورك ستفقد تقريبا كل خدماتها الهاتفية، على الأقل فترة. إن فقدان الخدمة الهاتفية كان سيؤثر في البنى الأساسية الأخرى، وكانت التأثيرات ستتوالى.

تتويجا للبيان الذي قدمه غرين[7]، عممت وكالة الاستخبارات المركزية - حيث كان بيل ستودمان هو القائم بأعمال المدير فترة وجيزة - تقريرا سريا حول أوجه الضعف والثغرات الأمنية لأنظمة «سكادا» SCADA. هذا الاسم المختصر يعني «منظومة التحكم الإشرافي وجمع البيانات» Supervisory Control and Data Acquisition. في جميع أرجاء البلاد، ومجددا لأسباب اقتصادية، فإن شركات المرافق العامة، ومحطات المياه، وخطوط السكك الحديدية، وهي قطاعات شاسعة من البنية الأساسية الحرجة البالغة الأهمية، كانت جميعها ترتبط قطاعا بالآخر من خلال شبكات الحاسوب، ويُتحكم فيها جميعا من بُعد، وفي بعض الأحيان بواسطة مراقبين بشريين، وغالبا باستخدام مستشعرات مؤللة. قبل تقرير وكالة الاستخبارات المركزية فإن بضعة أعضاء من مجموعة العمل لم يكونوا قد سمعوا قط بشأن منظومة «سكادا» SCADA. الآن أدرك الجميع أنهم على الأرجح كانوا فقط يخدشون سطحَ خطرٍ جديدٍ أتى مع التكنولوجيا الجديدة.

كتبت غوريليك مذكرة، محذرة رؤساءها من أن مجموعة العمل كانت تتوسع في نطاق استقصائها، «في ضوء اتساع[8] البنى الأساسية الحرجة وتعدد مصادر وأشكال الاعتداء». لم يعد يكفي النظر في احتمالية وتداعيات تفجير الإرهابيين البنايات الحرجة، كان يجب على المجموعة - في نهاية المطاف الرئيس - أن تنظر أيضا في «التهديدات التي تأتي من مصادر أخرى».

ما الاسم الذي يمكن أن نطلقه على تلك التهديدات «الأخرى»؟ كلمة واحدة كانت تحوم[9] في القصص والمقالات التي تدور بشكل أو بآخر حول القرصنة الحاسوبية (الاختراقات)؛ وهي كلمة «سيبر» (cyber). كان للكلمة جذورها في «السيبرنيطيقا» (cybernetics)، وهو مصطلح يعود إلى منتصف القرن التاسع عشر، يصف الحلقات المغلقة لأنظمة المعلومات. لكن في السياق الراهن لشبكات الحاسوب نشأ هذا المصطلح عن رواية «نيورومانسر» Neuromancer، رواية

الخيال العلمي التي كتبها ويليام جيبسون William Gibson في العام 1984، وهي قصة جامحة واستشرافية على نحو مخيف، تتناول القتل وأعمال الفوضى (التخريب) في عالم «الفضاء السيبراني» الافتراضي.

إن مايكل فاتيس Michael Vatis، المحامي بوزارة العدل وعضو مجموعة العمل الذي كان قد قرأ من فوره رواية جيبسون، كان هو من دعا إلى تبني هذا المصطلح. كان بقية الأعضاء معارضين، إذ إن المصطلح بدا به الكثير من الخيال العلمي، وكان عبثيا جدا وغير مقنع. لكن حالما تنطق الكلمة فإنها كانت ملائمة على نحو محكم. منذ تلك اللحظة فصاعدا كان أعضاء المجموعة، وغيرهم ممن درسوا المسألة، سيتحدثون بشأن «الجريمة السيبرانية» (cyber crime)، و«الأمن السيبراني» (cyber security)، و«الحرب السيبرانية» (cyber war).

ما الذي يمكن فعله حيال هذه التهديدات السيبرانية؟ كان هذا هو السؤال الفعلي، السبب الأساسي لوجود المجموعة، وهنا عجز أعضاء المجموعة. كان هناك العديد من القضايا التي تمس الكثير من الاهتمامات والاعتبارات البيروقراطية، والسياسية، والمالية، والمؤسسية؛ كانت أكثر وأكبر من أن تحسمها مجموعة عمل مشتركة بين الوكالات.

في 6 فبراير 1996 أرسلت غوريليك تقرير المجموعة إلى راند بيرز Rand Beers، مستشار كلينتون للاستخبارات، ونقطة الاتصال فيما يخص جميع القضايا المتعلقة بالتوجيه الرئاسي بشأن سياسة مكافحة الإرهاب (بي دي دي - 39) PDD-39، والذي كان قد حث على إنجاز هذه الدراسة. كانت النقطة الرئيسية في التقرير هي الإشارة إلى وجود نوعين من التهديدات للبنية الأساسية الحرجة، تهديدات مادية وأخرى سيبرانية، كانت هذه النقطة مبتكرة، بل تاريخية. أما فيما يخص خطة العمل، فقد لجأت المجموعة إلى أسلوب الإحالة المعتاد من مثل هذا النوع من فرق العمل حينما لا يعرفون ماذا عساهم أن يفعلوا. أوصى فريق العمل بتشكيل لجنة رئاسية.

على مدى فترة من الوقت، لم يحدث شيء. راند بيرز أخبر غوريليك أن تقرير مجموعتها كان قيد الدراسة، لكن لم تكن هناك متابعة. كانت هناك حاجة إلى حافز يحرك الأمور، وجدته غوريليك في شخصية سام نان Sam Nunn، الديموقراطي البارز عضو لجنة مجلس الشيوخ المعنية بالخدمات المسلحة.

كانت جوريليك تعرف نان منذ أيام عملها مستشارة عامة للبنتاغون. كلاهما كان من صقور الديموقراطيين، لم يكونا من سلالة نادرة، لكنهما أيضا ليسا من سلالة شائعة، وكانا يستمتعان بمناقشة القضايا معا. أخبرته جوريليك بشأن ما اكتشفته مجموعتها. استجابة لذلك، أدرج نان بندا في قانون إقرار الدفاع الوطني(*) في ذلك العام، مطالبا السلطة التنفيذية بأن تقدم إلى الكونغرس تقريرا بشأن سياسات وخطط درء الهجمات الحاسوبية على البنية الأساسية القومية.

أيضا، طلب نان من «مكتب المحاسبة العامة» General Accounting Office، وهي دائرة الرقابة على السلطة التشريعية، إجراء دراسة مماثلة. أعد مكتب المحاسبة العامة تقريره بعنوان «أمن المعلومات: الهجمات الحاسوبية في وزارة الدفاع تثير أخطارا متزايدة» Information Security: Computer Attacks at Department of Defense Pose Increasing Risks وفي أحد تقديراته، أشار التقرير إلى أن وزارة الدفاع «ربما شهدت ما يصل إلى 250 ألف اعتداء[10] خلال العام السابق»، وأن ثلثي تلك الهجمات كان ناجحا، وأن «عدد الهجمات يتضاعف كل عام، مع زيادة استخدام الإنترنت إلى جانب زيادة حنكة «قراصنة الحاسوب» (الهاكرز) وتطور أدواتهم.

لم يكن هذا الرقم مستبعدا فقط (ربع مليون اعتداء في العام يعني 685 اعتداء في اليوم، منها 457 نفاذا فعليا ناجحا)، ربما يكون هذا الرقم قد أتى من العدم بشكل عشوائي تماما، ومثلما أقر معدو التقرير أنفسهم، فإن ثمة «جزءا صغيرا» من الهجمات هو الذي كان «يُكتشَف ويُبلَغ عنه فعليا».

مع ذلك، بعثت الدراسة موجة صدمية عنيفة سرت خلال أروقة معينة. تأكدت جوريليك من أن بيرز كان على علم بأصداء الموجة، وحذرته من أن نان كان على وشك عقد جلسات استماع حول هذا الموضوع، وألمحت إلى أن الرئيس كان سيعمل بجد في مواجهة هذه العاصفة.

حدد نان يوم 16 يوليو موعدا لجلسة الاستماع. في يوم 15 يوليو، أصدر كلينتون الأمر التنفيذي الرقم 13010، لتشكيل اللجنة رفيعة المستوى التي كان

(*) «قانون إقرار الدفاع الوطني» National Defense Authorization Act هو اسم يطلق على كل سلسلة من القوانين الفدرالية للولايات المتحدة التي تحدد الموازنة والنفقات السنوية لوزارة الدفاع الأمريكية. [المترجم].

فريق عمل جوريليك قد اقترحها. كان الأمر التنفيذي يكاد يكون نسخة مطابقة للمسوَّدة المقترحة من مجموعة العمل قبل ذلك بثلاثة أشهر. استهل كلينتون الأمر التنفيذي بالقول: «إن بعض البنى الأساسية القومية[11] حيوية جدا، إلى درجة أن عجزها أو تدميرها سيكون له تأثير مدمر في الدفاع عن الولايات المتحدة أو في أمنها الاقتصادي»، وسرد قائمة القطاعات الثمانية «الحرجة» التي كان فريق العمل قد حددها. تابع الأمر التنفيذي: «تنقسم تهديدات هذه البنى الأساسية الحرجة إلى فئتين: تهديدات مادية للممتلكات الملموسة تهديدات مادية، وتهديدات من هجمات إلكترونية، أو باستخدام الترددات الراديوية، أو معتمدة على الحاسوب، تنقض على مكونات المعلومات أو الاتصالات التي تتحكم في البنى الأساسية الحرجة».

في اليوم التالي، عقدت لجنة الشؤون الحكومية في مجلس الشيوخ، حيث كان نان عضوا فيها باعتباره على رأس الديموقراطيين، جلسة استماع حول هذا الموضوع، تلك الجلسة التي طال انتظارها بشغف. كانت جايمي جوريليك هي أحد الشهود، وحذّرت قائلة: «ليس لدينا بعد هجوم سيبراني إرهابي[12] على البنية الأساسية، لكنني أعتقد أنها مسألة وقت فقط. نحن لا نريد أن ننتظر حدوث المعادل السيبراني لـهجوم «بيرل هاربور» Pearl Harbor[*]».

دخل العصر السيبراني رسميا إلى حيّز التنفيذ.

بالتالي - خلف الستار - كان عصر وسائل الحرب السيبرانية هو أيضا يمضي قدما. في أحد اجتماعات مجموعة عمل البنية الأساسية الحرجة، عمد ريتش ويلهلم إلى تنحية جايمي جوريليك جانبا، وبعبارات عامة فضفاضة أخبرها بشأن الوجه الآخر فائق السرية من التهديد الذي كانت تتقصى عنه، وهو أن ما نحن نفعله بدول أخرى منذ فترة طويلة، بدأت بعض تلك الدول، أو أناس فيها بأعينهم، يفعلونه بنا. نحن لم نكن نسطو على بنوكهم (مصارفهم) أو نسرق أسرارهم الصناعية، إننا لم نكن في حاجة إلى القيام بذلك. لكننا كنّا نستخدم أدوات سيبرانية، «هجمات إلكترونية،

(*) كان الهجوم على بيرل هاربور ضربة عسكرية مفاجئة حدثت في صباح يوم 7 ديسمبر 1941 من قبل القوات الجوية البحرية الإمبراطورية اليابانية ضد القاعدة البحرية للولايات المتحدة في بيرل هاربور بإقليم هاواي، وأدى ذلك الهجوم إلى دخول الولايات المتحدة في الحرب العالمية الثانية. [المترجم].

أو ترددات راديوية، أو هجمات تعتمد على الحاسوب» - مثلما كان سيحددها الأمر التنفيذي الذي أصدره كلينتون - للتجسس عليهم، واستكشاف شبكاتهم، وإعداد ساحة المعركة لمصلحتنا، في حالة ما إذا نشبت حرب في يوم من الأيام.

شدد ويلهلم على أمر مهم هو أن قدراتنا الهجومية السيبرانية ينبغي أن تبقى بعيدا عن النقاش، أو حتى التلميح إليها، عند مناقشة أوجه ضعفنا الأمني أمام القدرات الهجومية السيبرانية للدول الأخرى. كانت برامج أمريكا في هذا المجال[13] من بين الأسرار الأكثر إحكاما في مؤسسة الأمن القومي بأسرها.

حينما التقى راند بيرز نوابا من مختلف وزارات مجلس الوزراء لمناقشة الأمر التنفيذي الذي أصدره كلينتون، طرح جون وايت John White، نائب وزير الدفاع، الفكرة ذاتها على زملائه نواب الوزراء، بالنبرة الرسمية المهيبة ذاتها: لا يمكن لأحد أن يذكر القدرات الهجومية السيبرانية لأمريكا.

لم تكن الحاجة إلى التكتم هي السبب الوحيد لما أعقب ذلك من صمت بشأن الموضوع. لم يقل أحد حول الطاولة ذلك، لكن من الواضح أن الاعتراف ببراعة وتفوق أمريكا في مجال السيبرانية، في الوقت الذي تنتقد فيه براعة الآخرين، كان على أقل تقدير سيبدو أمرا مربكا.

استغرق الأمر سبعة أشهر لتبدأ اللجنة أعمالها. كان بيرز يخدم ثانية بوصفه رجل البيت الأبيض المكلف، وكان أول ما يتعين عليه فعله هو أن يجد مكانا يلتقي فيه المفوضون أعضاءَ اللجنة. لم تكن بناية المكتب التنفيذي القديم، القصر المجاور للبيت الأبيض، مجهّزة بقدر كافٍ من وصلات الحاسوب (هذا في حد ذاته هو تفسير للحالة المؤسفة لمدى التأهب لأزمة سيبرانية). جاهد جون دويتش John Deutch، المدير الجديد لوكالة الاستخبارات المركزية، لكي يعمل أعضاء اللجنة في مقر الوكالة في لانجلي، حيث كان يمكنهم الحصول على وصول آمن إلى أي شيء كانوا يحتاجون إليه. لكن المسؤولين في وزارات أخرى خشوا من أن هذا ربما يسبب العزلة، والاعتماد المفرط على أجهزة الاستخبارات. في نهاية المطاف، عثر بيرز على جناح مكتبي شاغر في بناية يمتلكها البنتاغون في أرلينغتون Arlington. ولترويج الفكرة، قدمت وزارة الدفاع عرضا بأن تتحمل كل النفقات وتقدم الدعم التقني.

ثم جاءت مسألة تسمية أعضاء اللجنة. كانت هذه مسألة حساسة ودقيقة. فكل حركة لبيانات الحاسوب في البلاد كانت تقريبا تتدفق من خلال شبكات مملوكة لشركات خاصة، كان ينبغي أن يكون لها رأي في مصيرها. أعد بيرز وموظفوه قائمة تضم عشر وزارات ودوائر فدرالية كانت ستتأثر بأي توصيات تخرج من هذا المشروع، وهي: الدفاع، والعدل، والنقل، والخزانة، والتجارة، والوكالة الفدرالية لإدارة الطوارئ، وبنك الاحتياطي الفدرالي، ومكتب التحقيقات الفدرالي، ووكالة الاستخبارات المركزية، ووكالة الأمن القومي. وقرر بيرز أن على كل رئيس وكالة أن يختار اثنين يفوضهما لعضوية اللجنة، أحدهما مفوض رسمي والآخر أحد التنفيذيين لدى مقاولي (متعهدي) القطاع الخاص. بالإضافة إلى نواب الوزراء المساعدين، كان سينضم أيضا مديرون أو نواب رؤساء تقنيون من شركات مثل «إيه تي آند تي» AT & T، و«آي بي إم» IBM، و«الباسيفيك للغاز والكهرباء» Pacific Gas & Electric، «الرابطة القومية لمفوضي هيئات تنظيم المرافق العامة» National Association of Regulatory Utility Commissioners.

كانت هناك مسألة أخرى حساسة ودقيقة. كان التقرير النهائي للجنة سيطرح باعتباره وثيقة عامة علنية، لكن أوراق عملها واجتماعاتها كانت ستُصنف على أنها سرية، كان سيتعين فحص المفوضين من أجل الحصول على تصاريح أمنية سرية تسمح بالاطلاع على الأسرار العليا، وكان ذلك أيضا سيستغرق وقتا.

أخيرا، كان على بيرز ونواب الوزراء اختيار رئيس للجنة. كانت هناك معايير أثبتت جدواها وفعاليتها لمثل هذا المنصب، منها أنه (غالبا هو) ينبغي أن يكون بارزا مرموقا، لكن غير مشهور، ونوعا ما على دراية بالموضوع المطروح على اللجنة، ولكن ليس خبيرا فيه، محترما، ودودا ومنفتحا، ولكن غير مثقل بجدول أعماله الخاص، شخص لديه وقت فراغ، ولكن ليس منبوذا أو أحمق. توصلوا إلى جنرال من فئة النجوم الأربعة متقاعد من سلاح الجو يدعى روبرت ت. مارش Robert T. Marsh.

كان توم مارش قد ارتقى عبر مراتب الجانب التقني لسلاح الجو، لا سيما في وسائل الحرب الإلكترونية. اختتم مارش حياته المهنية قائدا لقسم الأنظمة الإلكترونية في قاعدة هانزكوم الجوية في ولاية ماساتشوستس Massachusetts،

ثم قائدا لقيادة أنظمة سلاح الجو في قاعدة أندروز الجوية، بالقرب من واشنطن. كان مارش يبلغ من العمر 71 عاما. ومنذ تقاعده من الخدمة الفعلية، كان قد خدم في مجلس العلوم الدفاعية والطائفة الاعتيادية من مجالس إدارة المؤسسات. في ذاك الوقت، كان مارش مديرا لجمعية معونة سلاح الجو، وهي المنظمة الخيرية الرئيسية لسلاح الجو.

خلاصة القول، لقد بدا الرجل مثاليا.

اتصل جون وايت John White، نائب وزير الدفاع، بالجنرال مارش لسؤاله عما إذا كان على استعداد لخدمة الرئيس بتوليه رئاسة لجنة لحماية البنية الأساسية الحرجة. أجاب مارش بأنه غير متيقن تماما مما تعنيه «البنية الأساسية الحرجة»، لكنه سيكون سعيدا بأن يساعد.

استعدادا للقيام بالمهمة، قرأ مارش التقرير الذي أعدته مجموعة عمل جوريليك الخاصة بالبنية الأساسية الحرجة، وبدا التقرير صحيحا. تذكر مارش أيامه في هانزكوم في أواخر السبعينيات وأوائل الثمانينيات من القرن العشرين، حينما حشد سلاح الجو تقنيات جديدة في الطائرات المقاتلة من دون الاهتمام بأوجه الضعف والثغرات الأمنية التي ربما يبذرونها. كانت جميع التحديثات تعتمد على وصلات القيادة والسيطرة، والتي لم تكن تحتوي على تكرارات (ازدواجية) تحوطية مدمجة. وثمة بضعة ضباط مخضرمين تقنيا من طاقم عمل مارش حذروه من أنه إذا حدث خلل في الروابط (الوصلات)، فستصير الطائرة عاجزة ومعاقة، وبالكاد قادرة على الطيران، فضلا عن القتال.

لكن، كان مارش بعيدا عن العمليات اليومية طوال اثني عشر عاما، وهذا التركيز على السيبرانية كان جديدا تماما بالنسبة إليه. وللحصول على المشورة والتحقق من الواقع، اتصل مارش بزميل قديم كان يعرف عن شأن هذه القضايا أكثر من أي شخص آخر، وهو ويليس وير Willis Ware.

كان وير مسايرا لكل خطوة من ثورة الإنترنت منذ أن كتب، قبل ذلك بنحو ثلاثين عاما، بحثه الإبداعي حول الثغرات الأمنية لشبكات الحاسوب. كان وير لايزال يعمل في مؤسسة «راند» RAND، وكان عضوا في المجلس الاستشاري العلمي لسلاح الجو، حيث كان مارش قد تعرّف عليه، ووثق به. أكد وير لمارش أن تقرير جوريلك

على المسار الصحيح، وأن هذه قضية خطيرة وتتزايد يوما بعد يوم، إذ إن الجيش والمجتمع أصبحا أكثر اعتمادا على تلك الشبكات، وأن قلة قليلة من الناس كانوا يهتمون بهذا الأمر.

صار وير مفعما بالثقة بعد دردشته مع مارش. كان الأمر التنفيذي الذي أصدره الرئيس قد اعتمد اللجنة لفحص أوجه الضعف والثغرات الأمنية أمام التهديدات المادية والتهديدات السيبرانية. أدرك مارش أن الحلول الخاصة بالتهديدات المادية كانت إلى حد ما مباشرة وواضحة المعالم، أما التهديدات السيبرانية فهي التي كانت عنصرا حديثا، لذا فإن تركيزه كان سينصب عليها.

عقد مارش وأعضاء اللجنة اجتماعهم الأول في 14 فبراير من العام 1997. كان لديهم ستة أشهر لكتابة التقرير. كان بضعة أعضاء متبقين من مجموعة عمل البنية الأساسية الحرجة، وكان أبرزهم برنت غرين، مفوض البنتاغون، الذي كان بيانه عن الثغرات الأمنية لمبدّلات الاتصالات وخطوط شبكة الطاقة الكهربائية قد صدم بشدة جوريليك والآخرين. (جوريليك، التي تركت وزارة العدل في شهر مايو للاشتغال الحر في المحاماة، شاركت لاحقا في رئاسة هيئة استشارية للجنة، جنبا إلى جنب مع سام نان Sam Nunn).

كان معظم أعضاء اللجنة حديثي عهد بالقضايا المطروحة، وفي أحسن الأحوال، كانوا يعرفون قليلا بشأن أوجه الضعف والثغرات الأمنية في قطاعاتهم المتخصصة، لكن لم يكن لديهم أي فكرة عن أنها تمتد على نطاق واسع عبر كل القطاعات الاقتصادية الأخرى. وجميع ما اكتشفوه من بيانات في جلسات الإحاطة والاستماع، ملأهم بالجزع والهلع والشعور بالحاجة الملّحة.

كان مدير طاقم مارش ضابطا متقاعدا في سلاح الجو يدعى فيليب لاكومب Phillip Lacombe، وكان قد اكتسب سمعة طيبة بوصفه رئيسا لهيئة أركان في فريق يدرس أدوار ومهمات القوات المسلحة. كان إدراك لاكومب المفاجئ والمدهش للسيبرانية قد حدث صباح أحد الأيام، حينما كان هو ومارش على وشك الصعود إلى طائرة الساعة الثامنة صباحا متوجهة إلى بوسطن Boston، حيث كان من المقرر عقد جلسة استماع لهما في الساعة العاشرة والنصف. تأخرت رحلتهما ثلاث ساعات بسبب تعطّل نظام الحاسوب الخاص بخطوط الطيران، ولم يستطع أفراد

الطاقم تقدير الأوزان والاتزان (وهي مهمة كانت في السابق تتم باستخدام المسطرة الحاسبة المنزلقة(*)، التي لم يعد أحد حاليا يعرف كيفية استخدامها)، لذلك لم تتمكن الطائرة من الإقلاع. كانت المفارقة ساخرة بدرجة طاغية، هما كانا على وشك الذهاب لسماع إفادة بشأن تزايد اعتماد البلاد على شبكات الحاسوب، وهما لم يتمكنا من الوصول إلى هناك في الموعد المحدد بسبب اعتماد البلاد المتزايد على تلك الشبكات.

حينئذ أدرك لاكومب للمرة الأولى أن المشكلة امتدت إلى كل ركن من أركان الحياة العصرية. كان ضباط الجيش والمفكرون المعنيون بشؤون الدفاع يخشون أسلحة الدمار الشامل؛ الآن، رأى لاكومب أن هناك أسلحة عرقلة شاملة.

ومعظم جلسات الاستماع التي عقدتها اللجنة، فضلا على ما يسبقها وما يليها من مناقشات عرضية غير رسمية، كانت تتطرق مرارا وتكرارا إلى النقطة ذاتها. أفاد المسؤولون التنفيذيون في وول مارت Walmart(**) اللجنة بأنه أخيرا في يوم أحد، تعطل نظام الحاسوب الخاص بالشركة. نتيجة لذلك، لم يتمكنوا من فتح أي من متاجر التجزئة الخاصة بهم في منطقة جنوب شرق الولايات المتحدة. حينما أفاد أحد مديري شركة «باسيفيك للغاز والكهرباء» Pacific Gas & Electric، وهي واحدة من أكبر المرافق العامة في البلاد، بأن الشركة قد ربطت بالإنترنت جميع ما لديها من أنظمة التحكم، بهدف توفير المال وتسريع نقل الطاقة، سأله لاكومب عما تفعله الشركة بشأن الحماية الأمنية، لكنه لم يكن يعرف ما الذي يتحدث عنه لاكومب. كان العديد من أعضاء اللجنة يسأل رؤساء شركات السكك الحديد

(*) «المسطرة الحاسبة المنزلقة» slide rule هي أداة حاسبة تناظرية ميكانيكية، اخترعها في القرن السابع عشر عالم الرياضيات الإنجليزي القس ويليام أوتريد (1575 - 1660) William Oughtred، وهي تتكون من مسطرتين مدرجتين أو أكثر تنزلقان على المستوى نفسه، وتستخدم أساسا لإجراء عمليات الضرب والقسمة، وكذلك للمعادلات، مثل: الأسس، والجذور، واللوغاريتمات، وحساب المثلثات، ولكنها عادة لا تستخدم لإجراء عمليات الجمع أو الطرح. وعلى الرغم من تشابهها في الاسم والمظهر مع المسطرة النمطية، فإنها لا تستخدم لقياس الطول أو لرسم الخطوط المستقيمة. قبل ظهور الآلة الحاسبة الإلكترونية، كانت هي أداة الحساب الأكثر استخداما في العلوم والهندسة، واستمر استخدامها في النمو خلال الخمسينيات والستينيات من القرن العشرين حتى في أثناء إدخال الحواسيب تدريجيا؛ ولكن في العام 1974، وأمام الآلة الحاسبة الإلكترونية العلمية المحمولة باليد، فإنها بدت قديمة وقد عفّى عليها الزمن. [المترجم].

(**) «وول مارت» هي شركة أمريكية متعددة الجنسيات للبيع بالتجزئة تدير سلسلة من محال الهايبر ماركت، ومتاجر التخفيضات، ومحال البقالة. [المترجم].

وشركات الطيران بشأن كيفية ضمانهم أمن المبدّلات، والمسارات (السكك)، والجداول الزمنية، ورادارات الملاحة الجوية التي يُتحكم فيها اعتمادا على الحواسيب، وكانت القصة ذاتها لم تتغير، بدا رؤساء الشركات في حيرة. لم يكن لديهم أي فكرة أن الأمن كان مشكلة.

في 13 أكتوبر من العام 1997، أصدرت لجنة الرئيس لحماية البنية الأساسية، كما كان يُطلق عليها رسميا، تقريرها في 154 صفحة من النتائج والتحليلات والملاحق التقنية (الفنية) التفصيلية. نص التقرير في صفحاته الافتتاحية على: «تماما مثلما حدث في العصر النووي في النصف الأخير من القرن العشرين، ودعتنا الأسلحة الرهيبة بعيدة المدى[15] إلى التفكير بشكل مختلف بشأن الأمن. الآن، تدفعنا التكنولوجيا الإلكترونية لعصر المعلومات إلى اختراع وسائل جديدة لحماية أنفسنا. نحن ينبغي أن نتعلم كيفية التغلّب على جغرافيا جديدة، حيث تكون الحدود غير ذات أهمية، والمسافات غير ذات معنى، حيث يكون العدو ربما قادرا على الإضرار بالنظم الحيوية التي نعتمد عليها من دون أن يتواجه مع قوتنا العسكرية».

أضاف التقرير: «اليوم يمكن لحاسوب أن يتحكم في فتح وإغلاق المبدّلات أو الصمامات، وتحريك الأموال من حساب بنكي (مصرفي) إلى حساب آخر، أو نقل أمر عسكري لمسافة تصل إلى آلاف الأميال بذات سرعة نقله من الغرفة المجاورة، ومن مخبأ للإرهابيين بذات سهولة نقله من حجيرة مكتبية أو من مركز قيادة عسكري». كان يمكن لتلك «الهجمات السيبرانية» أن «تقترن مع هجمات مادية» في محاولة «لشل أو إثارة ذعر قطاعات كبيرة من المجتمع، وتدمير قدرتنا على الاستجابة للحوادث» (من خلال إعاقة نظام 911 أو اتصالات الطوارئ، على سبيل المثال)، وتعرقل قدرتنا على نشر القوات العسكرية التقليدية، وبخلاف ذلك تحد من حرية عمل قياداتنا الوطنية».

تحاشى التقرير التهويل والانهزامية، ولم يكن هناك حديث هنا بشأن «بيرل هاربر سيبرانية». صرح كاتبو التقرير في البداية بأنهم رأوا «أنه ليس هناك أي دليل على وجود هجوم سيبراني وشيك يمكن أن يسبب تأثيرا ضارا في البنى الأساسية الحرجة في البلاد». وعلى الرغم من ذلك، فإنهم قالوا: «هذا لا يعد تأسيسا للشعور بالرضا عن الذات أو للتراخي»، وأضافوا: «إن القدرة على الإيذاء - لا سيما من خلال

شبكات المعلومات - هي حقيقة واقعة، وهي تنمو بمعدل ينذر بالخطر، ونحن ليس لدينا سوى بضعة دفاعات في مواجهتها».

كان هذا بالكاد هو أول تقرير ينشر تلك التحذيرات، أما النتائج التي توصل إليها ويليس وير قبل ذلك بعقود، والتي اعتُمدت كسياسة (أو محاولة سياسة) في التوجيه الرئاسي السري المتعلّق بالأمن القومي (إن إس دي دي - 145) الذي أصدرته إدارة ريغان، فقد تغلغلت في الأوساط المحدودة للمسؤولين الرسميين من أصحاب التفكير التقني. في العام 1989، قبل ثمانية أعوام من تقرير الجنرال مارش، كان المجلس القومي للبحوث قد أصدر دراسة بعنوان «تنامي أوجه ضعف شبكات الاتصالات العمومية» Growing Vulnerability of the Public Switched Networks، حذَّرت من أن «تهديدا جادا خطيرا للبنية الأساسية للاتصالات[16] آخذ في التطور» من «عناصر طبيعية، أو عرضية، أو نزوية متهورة، أو عدائية».

بعد مضي عامين، أصدر المجلس ذاته تقريرا بعنوان «الحاسبات في خطر» Computers at Risk، ذكر أن «اللص المعاصر[17] يستطيع أن يسرق باستخدام الحاسوب أكثر مما يسرقه بالبندقية، وربما يكون إرهابيو الغد قادرين على إلحاق ضرر باستخدام لوحة مفاتيح أكثر من الضرر الذي يحدثونه باستخدام قنبلة».

في نوفمبر من العام 1996، قبل أحد عشر شهرا فقط من صدور تقرير مارش، كان فريق عمل تابع لمجلس علوم الدفاع بشأن الحماية من وسائل حرب المعلومات قد وصف «الاعتماد المتزايد»[18] على شبكات غير حصينة ومعرضة للخطر على أنها «مكونات في وصفة لكارثة أمن قومي». أوصى التقرير بأكثر من خمسين إجراء لاتخاذها على مدار الأعوام الخمسة اللاحقة، بتكلفة قدرها 3 مليارات دولار.

كان دوين أندروز Duane Andrews هو رئيس فريق العمل هذا، وكان في الآونة الأخيرة قد شغل منصب مساعد وزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات، همزة الوصل بين البنتاغون ووكالة الأمن القومي. كان نائب رئيس فريق العمل هو دونالد لاثام، الذي كان يشغل منصب مساعد وزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات قبل ذلك باثني عشر عاما، وحينها كان هو القوة الدافعة وراء التوجيه الرئاسي السري المتعلّق بالأمن القومي (إن إس دي دي - 145) الذي صدر في عهد ريغان، وهو كان أول توجيه

رئاسي بشأن أمن الحاسوب. كان أندروز في استهلاله متشككا - بقدر يصل إلى حد السخرية - من أن التقرير كان سيحدث أثرا، وكتب: «كان يتعين عليّ أن أشير أيضا إلى أن هذا هو العام الثالث على التوالي الذي تقدم فيها دراسة أو فريق عمل من مجلس علوم الدفاع توصيات مماثلة».

لكن خلافا لتلك الدراسات، كان تقرير مارش نتاج عمل لجنة رئاسية كان القائد الأعلى هو الذي قد أصدر أمرا بتشكيلها. كان أحد موظفيه سيقرأ تقريرها، وربما كان الرئيس ذاته سيطلع على الموجز التنفيذي. باختصار، كانت هناك فرصة أن تنبت سياسة من جذور التقرير.

على الرغم من ذلك، لم يحدث شيء فترةً ما، لا رد من الرئيس، ليس أكثر من لقاء أو صورة تذكارية مع رئيس اللجنة. بعد ذلك ببضعة أشهر، ألمح كلينتون بإيجاز إلى مضمون التقرير في كلمته في أثناء حفل تخرج في الأكاديمية البحرية، وقال: «في جهودنا لمكافحة[19] الإرهاب والهجمات السيبرانية والأسلحة البيولوجية، ينبغي لنا جميعا أن نكون بالغي الشراسة». كان هذا كل ما في الأمر، على الأقل في العلن أمام الناس.

لكن خلف الكواليس، وفي الوقت ذاته الذي كان فيه مارش وأعضاء اللجنة يختتمون جلسات الاستماع النهائية، كان البنتاغون ووكالة الأمن القومي يخططان لتدريب عالي السرية، محاكاة لهجوم سيبراني، كان ذلك التدريب سيبعث الحياة في تحذيرات مارش، وهو بالفعل في نهاية المطاف حث كبار المسؤولين على العمل واتخاذ التدابير المناسبة.

4

المُتَلَقِّي المُؤَهَّل

في 9 يونيو 1997[1] بدأ خمسة وعشرون عضوا من «الفريق الأحمر»(*) بوكالة الأمن القومي تدريبا أُطلق عليه اسم «المُتَلَقِّي المُؤَهَّل» (Eligible Receiver)، وكانت مهمتهم هي اختراق شبكات الحاسوب في وزارة الدفاع من دون استخدام معدات وبرمجيات سوى تلك المتاحة تجاريا في الأسواق. كان هذا هو أول

«كان تدريب «المُتَلَقِّي المُؤَهَّل» أول تدريب عالي المستوى لاختبار مدى جاهزية جيش الولايات المتحدة ومنشآته وقياداته المقاتلة العمومية لمواجهة هجوم سيبراني»

(*) بوجه عام «الفريق الأحمر» عبارة عن مجموعة مستقلة تتحدى منظمة ما بهدف تحسين فاعليتها من خلال افتراض دور أو وجهة نظر خصامية. عندما يستخدم هذا التعبير في سياق القرصنة الحاسوبية، فإن «الفريق الأحمر» هو مجموعة من القراصنة الأخلاقيين (قراصنة القبعة البيضاء) الذين يهاجمون البنية التحتية الرقمية للمؤسسة من أجل اختبار دفاعاتها. يتيح استخدام الفرق الحمراء السيبرانية «عمليات محاكاة للهجوم في العالم الحقيقي مصممة لتقييم وتحسين فعالية برنامج أمان المعلومات بالكامل». تستخدم وزارة الدفاع الأمريكية فرقا حمراء سيبرانية لإجراء تقييمات لشبكاتها الخاصة. هذه الفرق الحمراء معتمدة من قبل وكالة الأمن القومي ومن القيادة الاستراتيجية للولايات المتحدة، ويسمح هذا الاعتماد لهذه الفرق الحمراء بإجراء التقييمات العدائية على الشبكات التشغيلية في وزارة الدفاع، واختبار ضوابط الأمن المطبقة وتحديد نقاط الضعف في نظم المعلومات. [المترجم].

تدريب عالي المستوى لاختبار مدى جاهزية قادة جيش الولايات المتحدة، ومنشآته، وقياداته المقاتلة العمومية لمواجهة هجوم سيبراني. كانت النتيجة مثيرة للقلق.

كان تدريب «المتلقي المؤهل» من بنات أفكار كينيث مينيهان Kenneth Minihan، وهو جنرال من فئة ثلاثة نجوم في سلاح الجو؛ قبل ذلك بأقل من عام ونصف العام، كان مينيهان قد خلف مايك ماكونيل مديرا لوكالة الأمن القومي. وقبل ذلك بستة أشهر، في أغسطس 1995، كان قد شغل منصب مدير وكالة استخبارات الدفاع، تتويجا لمسيرته المهنية في الاستخبارات العسكرية. لم يكن مينيهان يرغب في الانتقال إلى «فورت ميد»، لا سيما بعد تلك الفترة القصيرة التي قضاها في وكالة استخبارات الدفاع. لكن وزير الدفاع أصرّ، كانت قيادة وكالة الأمن القومي أكثر أهمية، مثلما قال، وكانت البلاد في حاجة إلى مينيهان على رأسها.

كان وزير الدفاع هو بيل بيري Bill Perry، عالم الأسلحة الذي كان - في أثناء إدارة كارتر - قد ابتكر وعرَّف مصطلح «وسائل الحرب المضادة للقيادة والسيطرة»، سلف «وسائل حرب المعلومات». قبل ذلك، وباعتباره الرئيس المؤسس لشركة «إيه إس إل» ESL, Inc، كان قد اضطلع ببناء العديد من الأجهزة والأدوات التي كانت وكالة الأمن القومي تستخدمها لإرساء الأساس لهذا النوع من وسائل الحرب.

منذ انضمامه إلى إدارة كلينتون، نائبا لوزير الدفاع، ثم وزيرا للدفاع، كان بيري يراقب وكالة الأمن القومي من كثب، ولم يعجبه ما رآه. كان العالم على نحو سريع يتحول إلى الرقمية والإنترنت، لكن بؤرة اهتمام وكالة الأمن القومي كانت لاتزال هي دوائر الهاتف وإشارات الموجات الميكروية. كان ماكونيل قد حاول إحداث تغييرات لكنه فقد التركيز في أثناء هوسه بمشروع «رقاقة كليبر».

قال بيري لمينيهان: «إنهم محطمون هناك، ويجب عليك الذهاب لإصلاح الأمور».

كان مينيهان يتمتع بشهرة بوصفه يفكر تفكيرا ابتكاريا «خارج الإطار التقليدي»، وفي معظم الأوساط العسكرية لم يكن هذا الأمر يُنظر إليه على أنه أمر جيد، لكن بيري كان يعتقد أن لديه الأسلوب الصحيح والملائم ليهز «فورت ميد» ويحدث فيها تغييرا جذريا شاملا.

طوال فترة ستة عشر شهرا مصيرية حاسمة، من يونيو 1993 حتى أكتوبر 1994، كان مينيهان قائدا في قاعدة «كيلي» الجوية، التي تمتد عبر نطاق ضيق (جيب سياسي)

يسمى «تل الأمن» Security Hill، في أطراف مدينة سان أنطونيو San Antonio بولاية تكساس Texas، مقر مركز سلاح الجو لوسائل حرب المعلومات. منذ العام 1948، أي قبل أربعة أعوام من إنشاء وكالة الأمن القومي، كانت قاعدة «كيلي» - تحت أسماء مختلفة - هي حيث كان سلاح الجو يصنع رموز شفرته ويفك شفرة الخصوم.

في صيف العام 1994 أمر الرئيس كلينتون جنرالاته بالبدء في التخطيط لغزو هايتي. وعلى نحو ما كان مخوَّلا في قرار مجلس الأمن التابع للأمم المتحدة، كان الهدف هو طرد الحكام الديكتاتوريين الذين كانوا قد وصلوا إلى السلطة عن طريق قلب نظام الحكم، واستعادة حكم النظام الديمقراطي لرئيس الجزيرة المنتخب جان-برتران أريستيد Jean-Bertrand Aristide. كان ذلك الغزو سيشتمل على عدة محاور، قوات عمليات خاصة متمركزة مسبقا داخل البلاد، وقوات مشاة تنساب إلى الجزيرة من عدة ممرات، وحاملات طائرات في البحر الكاريبي لتقديم الدعم البحري. كانت مهمة مينيهان تتمثل في التوصل إلى أسلوب تستخدمه طائرات الولايات المتحدة، حاملات الجنود والقاذفات، ليمكنها - إذا لزم الأمر - التحليق فوق هايتي من دون اكتشافها.

كان لدى مينيهان في مركز وسائل حرب المعلومات، ضابط صغير ناشئ، كان فتى نابغا تقنيا، لا يختلف عن الشخصية التي جسدها ماثيو برودريك في فيلم «ألعاب الحرب (المناورات الحربية)»، وقد كان في شبابه محترفا في استخدام برمجية «عفريت الاتصال الهاتفي»، وكان يعبث مع شركة الهاتف محاكيا بعض نغمات طنين طلب الاتصال الهاتفي (Dial Tone)، وبذلك كان يستطيع إجراء اتصالات هاتفية دولية بالمجان. إزاء مشكلة هايتي، أتى الفتى إلى مينيهان بفكرة. كان قد أجرى بعض الأبحاث، واتضح أن نظام الدفاع الجوي في هايتي كان موصولا بخطوط الهاتف المحلية، وهو كان يعرف كيف يجعل كل الهواتف في هايتي مشغولة في آن واحد. لن تكون هناك حاجة إلى مهاجمة بطاريات الصواريخ المضادة للطائرات بالقنابل أو الصواريخ، الأمر الذي ربما يؤدي إلى تشريد وقتل المدنيين. كل ما كان على مينيهان وطاقمه الاضطلاع به هو عرقلة خطوط الهاتف.

في النهاية تقرر إلغاء الغزو. أرسل كلينتون وفدا رفيع المستوى ضم جيمي كارتر وكولين باول وسام نان لتحذير الحكام الديكتاتوريين المستبدين في هايتي

من الغزو الوشيك، ولاذ الحكام الطغاة بالفرار، وعاد أريستيد إلى السلطة من دون إطلاق رصاصة واحدة. لكن مينيهان كان قد أدرج فكرة «عفريت الاتصال الهاتفي» في الخطة الرسمية للحرب. إذا كان الغزو قد مضى قدما، فهذه هي الطريقة التي ستراوغ بها الطائرات الأمريكية لتتجنب النيران.

منذ اللحظة الأولى كان بيل بيري يرصد ويتابع خطة الحرب، وحينما علم بشأن فكرة مينيهان لمعت عيناه. كان لها صدى مع طريقة تفكيره بوصفه رائدا في التدابير الإلكترونية المضادة. كانت خطة الإغراق الهاتفي في هايتي هي ما سلطت الأضواء على مينيهان، وجعلته يحظى باهتمام بيري باعتباره ضابطا ينبغي متابعته، وحينما أصبح الموقع المناسب شاغرا، دفع به بيري إليه.

ثمة شيء آخر جذب انتباه بيري بشأن قاعدة «كيلي» الجوية. لم يكن المركز قد ابتدع مخططات ونظما بارعة للغارات الهجومية على الخصوم فقط؛ لكنه أيضا، وفي وحدة مستقلة، ابتكر أسلوبا بارعا لاكتشاف، ورصد، وإبطال مفعول هجمات وسائل حرب المعلومات التي ربما يشنها الخصوم على أمريكا. لم يكن أي من الأفرع العسكرية الأخرى، ولا حتى سلاح البحرية، قد صمم أي شيء على هذا القدر من الفعالية.

كان هذا الأسلوب المبتكر يسمى «رصد أمن الشبكات»، وكان من اختراع عالم حواسيب في جامعة كاليفورنيا في ديفيس Davis اسمه تود هيبيرلين Todd Heberlein.

في أواخر ثمانينيات القرن العشرين ظهرت قرصنة الحواسيب (اختراق الحواسيب) على أنها مصدر إزعاج وضرر خطير، وتهديد عرضي من حين إلى آخر. حدثت أول حالة مرعبة كالكابوس[2] في 2 نوفمبر 1988، حينما تعطل نحو ستة آلاف حاسوب يونكس UNIX، أي نحو 10 في المائة من الحواسيب الموصولة بشبكة الإنترنت، وتضمن ذلك حواسيب قاعدة «رايت - باترسون» الجوية، ومختبر الجيش الميداني (القوات البرية) لأبحاث الأسلحة البالستية (التسيارية)، والعديد من منشآت وكالة الفضاء الأمريكية (ناسا)؛ وبدت الحواسيب ميتة، وبقيت كذلك طوال خمس عشرة ساعة، بسبب إصابة أتتها من أحد المصادر الخارجية، وكانت يستعصي علاجها. كانت تلك الإصابة قد أطلق عليها اسم «دودة موريس» Morris Worm، على اسم الجاني مقترف الجريمة، وهو كان طالبا في الدراسات العليا بجامعة «كورنيل» يدعى روبرت ت. موريس الابن Robert T. Morris Jr (هذا ما أوقع «فورت ميد» في

حرج، تبين أنه ابن روبرت موريس الأب Robert Morris Sr، كبير علماء مركز أمن الحاسوب في وكالة الأمن القومي، وكان مركز أمن الحاسوب هو الذي يتعقب ذلك الفيروس الحاسوبي المتنقل (الدودة الحاسوبية) لمعرفة الجاني).

لم يكن موريس قد قصد أي ضرر. كان قد بدأ في اختراق شبكة الإنترنت مستخدما عدة مواقع جامعية كبوابة لإخفاء هويته، لا لسبب إلا لقياس مدى اتساع الشبكة (في ذلك الوقت، لم يكن أحد يعرف مدى اتساعها)، لكنه ارتكب خطأ جسيما، كان الفيروس الحاسوبي المتنقل (دودة الحاسوب) يرسل استفساره إلى عدة حواسيب على نحو متكرر (لم يكن موريس قد برمجه ليتوقف حالما يتلقى ردا)، مما أدى إلى تحميل الأنظمة فوق طاقتها وانهيارها. في أعقاب الفيروس الحاسوبي المتنقل (دودة الحاسوب) استنبط العديد من علماء الحاسوب وبعض المسؤولين درسا مرعبا، كان موريس قد كشف مدى سهولة تعطيل النظام وإيقاف تشغيله، لو كانت هذه هي نيته فقد كان سيمكنه إحداث أضرار أكبر بكثير.

نتيجة لهجوم «دودة موريس»، طوَّر بعض علماء الرياضيات برامج للكشف عن المتسللين، لكن تلك البرامج كانت مصممة لحماية حواسيب منفردة غير متصلة بشبكة. كان ابتكار تود هيبيرلين[3] يكمن في تصميم برمجية لكشف التسلل يمكن تنصيبها على شبكة مفتوحة، ويمكن توصيل أي عدد من الحواسيب بها. كانت برمجيته تعمل على عدة مستويات. أولا، كانت تتحقق من وجود نشاط شاذ على الشبكة؛ على سبيل المثال، كلمات مفتاحية تشير إلى أن شخصا ما كان ينفذ محاولات متكررة لتسجيل الدخول إلى حساب، أو أنه كان يجرب كلمات مرور عشوائية الواحدة تلو الأخرى. على نحو خاص كانت مثل هذه المحاولات تسترعي الانتباه إذا دخلت إلى الشبكة من عنوان MIT.edu الذي يخص «معهد ماساتشوستس للتكنولوجيا»، نظرا إلى أن المعهد كان معروفا عنه السماح لأي شخص وكل شخص بالولوج إلى وحداته الطرفية عن طريق الاتصال الهاتفي من أي مكان على شبكة الإنترنت، ومن ثم كان نقطة مفضلة لدخول قراصنة الحاسوب (الهاكرز). كانت الأنشطة الشاذة غير السوية ستطلق تنبيها؛ وعند تلك النقطة، كان بإمكان البرمجية تتبع البيانات من جلسة عمل مخترق الحاسوب (الهاكر) في أثناء اتصاله بالشبكة، وتدوين عنوان الشبكة الخاص به، ومدة بقائه داخل الشبكة، وكم البيانات التي كان يستخلصها منها أو ينقلها إلى موقع

آخر (أطلق على «بيانات الجلسات» session data لاحقا اسم «البيانات الواصفة» metadata). بعد هذه المرحلة أثارت جلسات عمل مخترق الحاسوب (الهاكر) ما يكفي من الارتياب الذي يستوجب مزيدا من الاستجلاء والتدقيق، كان بإمكان برمجية هيبيرلين تتبع كامل محتويات بيانات الجلسات، بما في ذلك ما كان مخترق الحاسوب (الهاكر) يفعله، وما كان يقرأه، وما الذي أرسله، كل ذلك لحظيا في الوقت الحقيقي، وعبر كامل الشبكة التي تراقبها البرمجية.

مثل العديد من قراصنة الحاسوب (الهاكرز) ومناهضيهم المعاصرين، كان هيبيرلين ملهما بكتاب «بيضة طائر الوقواق» The Cuckoo's Egg الذي كتبه كليف ستول Cliff Stoll في العام 1989 (كان ضابطا صغيرا[4] ساعد على مواءمة برمجية هيبرلين في مركز سلاح الجو لوسائل حرب المعلومات، وكتب بحثا بعنوان «50 درسا من أول 50 صفحة من كتاب بيضة طائر الوقواق»). كان «ستول» هيبيًّا(*) عبقريا، وفلكيا بارعا، يعمل في «مختبر لورانس بيركلي القومي»، كمسؤول نظام الحاسوب. في أحد الأيام، اكتشف ستول خطأ في فاتورة هاتف المختبر يبلغ خمسة وسبعين سنتا؛ وبدافع الفضول المحض، تعقب مصدر الخطأ، وانتهى به الأمر إلى الكشف عن حلقة تجسس من ألمانيا الشرقية تحاول سرقة أسرار عسكرية تخص الولايات المتحدة، مستخدمة الموقع المفتوح الخاص بمختبر «بيركلي» كمنفذ. على مدى عدة أشهر تالية، معتمدا كليةً على دهائه وخبرته، اخترع ستول أساليب لكشف التسلل، صارت معتمدة وجرى تبنيها على نطاق واسع على مدار العقود الثلاثة التالية. ألحق ستول طابعة بخطوط الولوج إلى نظام الحاسوب الخاص بالمختبر، بحيث تدون سجلا بأنشطة المهاجم. وبرفقة أحد زملائه في «بيركلي» يدعى لويد بيلناب Lloyd Bellknap، بنى «محلل منطق» logic analyzer وبرمجه لتتبع مستخدم بعينه. وحينما كان يسجل المستخدم الدخول، كان أحد الأجهزة يرسل تلقائيا استدعاء إلى ستول من خلال جهاز النداء(**)، الذي كان بدوره سيسارع إلى المختبر. كان «محلل المنطق» سيضاهي أيضا سجلات مواقع أخرى كان مخترق الحاسوب (الهاكر) قد

(*) الهيبيون Hippies: صفة يُعرف بها فتيان يرفضون القيم الاجتماعية في مجتمع الاستهلاك الصناعي. [المترجم].
(**) جهاز النداء pager أو beeper هو جهاز اتصال لاسلكي صغير الحجم يستقبل ويعرض الرسائل النصية أو الصوتية القصيرة، قلَّ استخدامه ويعتبر شبه معدوم بعد ظهور الهاتف الجوال. [المترجم].

تسلل إليها، بذلك كان ستول يستطيع أن يستنبط صورة كاملة لما كان يسعى إليه مخترق الحاسوب (الهاكر).

حدَّث هيبيرلين تقنيات ستول، حتى إنه كان يستطيع تعقب وصد من يخترق ليس فقط «مودم» واحدا منفردا، ولكن أيضا من يخترق شبكة حاسوبية.

كان ستول مصدر إلهام عمل هيبرلين بمعنى آخر مختلف. بعد أن اكتسب ستول شهرة بسبب اصطياده قراصنة الحاسوب (الهاكرز) الألمان الشرقيين، واستحق كتابه أن يدرج على قائمة الكتب الأفضل مبيعا، فإن «مختبر لورنس ليفرمور القومي»، المختبر الأكثر ميلا إلى العسكرية، الذي كان يبعد أربعين ميلا عن «بيركلي»، استغل العناوين الرئيسية للصحف وطلب تمويلا من وزارة الطاقة لإنشاء نظام «رصد أمن الشبكة». فاز مختبر ليفرمور بالعقد، لكن لم يكن لديه أحد يعرف كيفية بناء مثل هذا النظام. تواصل مديرو المختبر مع كارل ليفيت Karl Levitt، الأستاذ الجامعي في علوم الحاسوب بجامعة كاليفورنيا في ديفيس. أحضر ليفيت معه تلميذه النجيب المجتهد تود هيبيرلين.

بحلول العام 1990 كان «مركز سلاح الجو لدعم التشفير» (الذي صار بعد بضعة أعوام جزءا من مركز سلاح الجو لوسائل حرب المعلومات) يطور نظام كشف التسلل الخاص به. بعد الفيروس الحاسوبي المتنقل المسمى «دودة موريس»، بدأ المتخصصون في مجال التكنولوجيا في تنصيب أنظمة «كشف الهجوم المعتمدة على المضيف» (host-based attack-detection)، الوسيلة المفضلة في تلك الأيام، التي كان يمكن أن تحمي جهاز حاسوب منفردا، لكن سرعان ما اعتبرت قاصرة وغير كافية. كان بعض الاختصاصيين قرأوا بشأن برمجية هيبرلين لرصد أمن الشبكات، وكلفوه بمواءمتها وفقا لاحتياجات المركز.

في غضون عامين أعاد خبراء الشفرة تسمية برمجيته إلى «نظام القياس المؤلل للحوادث الأمنية (أيه إس آي إم)» Automated Security Incident Measurement (ASIM)، ونصّبوها على شبكات سلاح الجو. أُنشئ قسم جديد في مركز سلاح الجو، أُطلق عليه اسم «فريق الاستجابة لحالات طوارئ الحاسوب» (Computer Emergency Response Team)، لتشغيل وإدارة البرمجية، وتعقب المتسللين، وإحاطة الجهات العليا علما في حالة حدوث اختراق جاد وخطير.

كان الفريق يستطيع مراقبة شبكات سلاح الجو في جميع أنحاء البلاد من داخل حجيراتهم في سان أنطونيو، أو تلك كانت الفكرة على أي حال.

كان البرنامج يواجه عقبات بيروقراطية منذ البداية. في 7 أكتوبر 1992 كتب روبرت مولر Robert Mueller، مساعد المدعي العام المسؤول عن القسم الجنائي بوزارة العدل، خطابا يحذر فيه من أن رصد الشبكة ربما ينتهك القوانين الفدرالية التي تنظم التنصت على الاتصالات. كانت الوسيلة التي تُرصد بها الشبكة لا بد أن تلتقط أيضا حركة تدفق المعلومات عبر الإنترنت لبعض المدنيين الأبرياء. أشار مولر إلى أن هذه الممارسة ربما تكون غير مشروعة. كانت القوانين المنظمة للتنصت قد صيغت قبل عصر قراصنة الحاسوب (الهاكرز) وفيروساته. لم تكن أي محكمة قد أصدرت قرارا بعد بشأن تطبيقاتها واستخداماتها الراهنة. لكن مولر كتب أنه ريثما يصدر مثل هذا القرار، يجب على جميع الدوائر الفدرالية التي تستخدم هذه التقنيات أن تنشر «لافتة تحذيرية»[5]، لتوجيه إشعار إلى «المتسللين غير المصرح لهم» بأنهم يخضعون للمراقبة.

تجاهل ضباط سلاح الجو في سان أنطونيو خطاب مولر، لأنه لم يكن أمرا بالتوقف والكف عن المراقبة. إضافة إلى ذلك فإن تحذير قراصنة الحاسوب (الهاكرز) من أنهم يخضعون للمراقبة كان سيدمر المغزى الأساسي من المراقبة.

بعد ذلك بعام واحد تلقى هيبرلين اتصالا هاتفيا من أحد مسؤولي وزارة العدل. في البداية حبس هيبرلين أنفاسه، متسائلا عما إذا كان الفدراليون في نهاية المطاف آتين للنيل منه. على النقيض من ذلك اتضح أن الوزارة كانت قد نصّبت أخيرا برمجيته، وكان المسؤول لديه سؤال تقني حول إحدى خصائص البرمجية. كانت وزارة العدل قد غيرت نبرتها، وتكيفت مع العالم الجديد بسرعة كبيرة. وفي مفارقة شديدة صار روبرت مولر في وقت لاحق مديرا لمكتب التحقيقات الفدرالي، وبلا هوادة استخدم برمجية رصد الشبكات لتعقب المجرمين والإرهابيين.

مع ذلك في مطلع الحقبة الجديدة طرح مولر سؤالا منطقيا مشروعا، هل كان مشروعا أن تراقب الحكومة الشبكة التي لم تكن تنقل اتصالات الأشرار من الأجانب فقط، بل كانت تنقل أيضا اتصالات عامة الأمريكيين؟ لقد طرحت هذه المسألة مجددا بعد ذلك بعشرين عاما، وبشغف زائد وجدل أوسع، حينما سرَّب أحد مقاولي (متعهدي) وكالة الأمن القومي، ويدعى إدوارد سنودن Edward Snowden، كنزا

دفينا من الوثائق فائقة السرية تحتوي على شرح تفصيلي لبرنامج الوكالة الموسع الهائل الخاص بالبيانات الواصفة.

إن أشد معارضة واجهتها برمجية رصد الشبكة في بداياتها، جاءت من سلاح الجو ذاته. في أكتوبر 1994 نُقل مينيهان من قاعدة كيلي الجوية إلى البنتاغون، حيث تولى منصب استخبارات سلاح الجو. جاهد مينيهان هناك بشدة من أجل اعتماد البرمجية وتبنيها على نطاق أوسع، لكن التقدم كان بطيئا. كانت الخدمات الحاسوبية في سلاح الجو ما يزيد قليلا على المائة نقطة للولوج إلى شبكة الإنترنت. وبعد ذلك بعامين حينما غادر مينيهان البنتاغون[6]، كانت فرق الحاسوب في سان أنطونيو قد تلقت الإذن برصد ست وعشرين نقطة منها فقط.

لم تكن الراصدات فقط هي التي كان مينيهان قد يواجه صعوبة بشأنها من أجل الحصول على قبول كبار الضباط، بل أيضا كان صميم موضوع أمن الحاسوب ذاته. أخطر مينيهان جنرالات من فئة النجوم الثلاثة والأربعة بشأن خطة عرقلة خطوط الهاتف في هايتي، مضيفا أن فرقه السابقة في سان أنطونيو كانت تستحدث وتبتدع عمليات مماثلة ضد حواسيب العدو. لم يكن أحد مهتما، كان معظم الجنرالات قد تدرجوا في المناصب كطيارين على الطائرات المقاتلة أو على قاذفات القنابل، ووفقا لأسلوب تفكيرهم، كانت أفضل طريقة لتعطيل أحد الأهداف هي إسقاط قنبلة عليه. لم يكن اختراق وصلات الحاسوب موثوقا به ويعول عليه، كما أن قياسه كان أمرا غير ممكن، وكانت تفوح منه رائحة «القوة الناعمة». وعلى الرغم من أن الجنرال كولن باول كان قد أصدر مذكرة حول وسائل حرب المعلومات، فإنهم لم يقتنعوا بها.

كان سلاح الجو المحبب لدى مينيهان يتحرك ببطء شديد، وكان متقدما كثيرا عن الجيش الميداني (القوات البرية) وسلاح البحرية في هذا المجال. لقد كان لإحباطه مستويان، كان يرغب في أن يعرف الجيش - الأفرع الثلاثة الرئيسية، بالإضافة إلى القيادة المدنية في البنتاغون - مدى براعة رجاله في اختراق شبكات الخصوم، ورغب في أن يدركوا الكيفية التي كانت بها شبكاتهم الخاصة مفتوحة على مصاريعها ليخترقها الخصوم أنفسهم.

بوصفه المدير الجديد لوكالة الأمن القومي، عقد مينيهان العزم على استخدام المنصب لإظهار مدى حسن تلك الأمور وسوئها.

كانت هيئة الأركان المشتركة في البنتاغون تجري تدريبا في كل عام يسمى «المتلقِّي المؤهَّل» Eligible Receiver، وهو محاكاة أو مناورة حربية مصممة لتسليط الضوء على أحد التهديدات أو إحدى الفرص التي كانت تلوح في الأفق. كان أحد التدريبات التي جرت أخيرا قد ركز على خطر الأسلحة البيولوجية. أراد مينيهان أن يكون التدريب التالي لاختبار أوجه ضعف شبكات الولايات المتحدة العسكرية في مواجهة الهجمات السيبرانية. كانت الطريقة الأكثر إثارة للقيام بذلك، والتي اقترحها مينيهان، هي شن هجوم حقيقي على تلك الشبكات بواسطة فريق من متخصصي استخبارات الإشارة (سيجينت) في وكالة الأمن القومي.

جاءت الفكرة إلى مينيهان من تدريب عسكري، كان في ذلك الحين في طور التنفيذ بالفعل، متضمنا الحلفاء الخمسة الناطقين بالإنجليزية - الولايات المتحدة، وبريطانيا العظمى، وكندا، وأستراليا، ونيوزيلندا - المعروفين في دوائر وكالة الأمن القومي باسم العيون الخمس، لاتفاقهم الرسمي على تشارك المعلومات الاستخباراتية فائقة السرية. كان هدف التدريب هو اختبار معدات جديدة للقيادة والسيطرة، كان بعضها لايزال في طور البحث والتطوير. كجزء من هذا الاختبار، كان طاقم مكون من ثمانية أفراد سيحاول اختراق المعدات، كان ذلك الطاقم يسمى فريق تقييم مواطن ضعف التحالف، وكان يعمل من وكالة نظم معلومات الدفاع في مقاطعة أرلينغتون Arlington بولاية فرجينيا Virginia. علم مينيهان أن قراصنة الحاسوب (الهاكرز) كانوا دائما يحققون النجاح.

كان مدير فريق التقييم مدنيا (غير عسكري) أمريكيا يدعى مات ديفوست Matt Devost، وكان يبلغ من العمر ثلاثة وعشرين عاما، تخرج حديثا في كلية سان مايكل في مدينة بيرلينغتون Burlington بولاية فيرمونت Vermont، حيث كان قد درس العلاقات الدولية وعلوم الحاسوب. في بدايات سن المراهقة، كان ديفوست يعمد إلى القرصنة الحاسوبية (هاكر) بغرض التسلية، وكان هو وأصدقاؤه من محبي التكنولوجيا قد شاهدوا فيلم ألعاب الحرب (المناورات الحربية) عدة مرات، ويتنافسون على اختراق مخدمات وكالة الفضاء الأمريكية (ناسا) وغيرها من الوكالات شبه العسكرية. وحينذاك، كان ديفوست يجلس في حجرة مكتب مع العديد من الغرباء المتقاربين فكريا، ليخترق أحد الأنظمة

الأكثر سرية في العالم، ثم يطلع جنرالات من فئة النجمتين والنجمات الثلاث بشأن ثغراتهم الأمنية التي يمكن استغلالها، وكل ذلك تحت اسم تعزيز الدفاعات الأمريكية والحليفة.

في آخر مناورة حربية أجراها التحالف، كان فريق ديفوست قد أوقف تشغيل أنظمة القيادة والسيطرة الخاصة بثلاثة عناصر من المشاركين، هم: كندا، وأستراليا، ونيوزيلندا؛ وسيطروا على الحاسوب الشخصي الخاص بالقائد الأمريكي، وأرسلوا إليه رسائل بريد إلكتروني وهمية خادعة، ومعلومات زائفة مضللة، مما أدى إلى تشويه منظوره بشأن ساحة المعركة، ودفعه إلى اتخاذ قرارات سيئة، كان يمكن في حرب حقيقية أن تعني الهزيمة.

كانت لدى وكالة الأمن القومي مجموعة مماثلة تسمى الفريق الأحمر، كانت جزءا من مديرية ضمان المعلومات (التي كانت تُعرف سابقا باسم مديرية أمن المعلومات)، الجانب الدفاعي من وكالة الأمن القومي، وكانت متمركزة في فانيكس FANEX، البناية التي تقع بالقرب من مطار فريندشيب (الصداقة) Friendship Airport. كان الفريق الأحمر في أثناء تدريباته البالغة الحساسية يعمل من داخل غرفة تسمى الحفرة The Pit، التي كانت مصنفة على أنها سرية جدا، حتى أنه لم يكن يعلم بوجودها سوى بضعة أشخاص في وكالة الأمن القومي، ولم يكن حتى في استطاعتهم الدخول إليها من دون المرور أولا عبر بابين موصدين بأقفال ذات أرقام سرية مركبة. كانت مهام عمل الفريق الأحمر الاعتيادية تتضمن استكشاف أوجه الضعف والثغرات الأمنية في الأجهزة أو البرمجيات الجديدة التي كان يجري تصميمها لوزارة الدفاع، وأحيانا لمصلحة وكالة الأمن القومي ذاتها. كان يتعيَّن أن ترقى تلك الأنظمة إلى مستوى مرتفع[7] حتى يتسنى اعتبارها آمنة بما يكفي لأن تشتريها الحكومة وتنصبها. وكانت مهمة الفريق الأحمر هي اختبار التأكد من أن تلك النظم تحقق هذا المستوى المرتفع.

كانت فكرة مينيهان هي استخدام الفريق الأحمر التابع لوكالة الأمن القومي بالطريقة ذاتها التي كانت دول العيون الخمس تستخدم بها فريق تقييم مواطن ضعف التحالف. لكن بدلا من وضعه في مناورة حرب محدودة النطاق، كان مينيهان يرغب في كشف الثغرات الأمنية في وزارة الدفاع كلها. إنه كان طوال أعوام قد حاول

إيضاح هذه النقطة لزملائه من كبار الضباط. وحاليا كان مينيهان يريد إثارة القضية لدى كبار المسؤولين في البنتاغون.

أعجب بيل بيري بالفكرة. مع ذلك استغرق الأمر من مينيهان عاما للقفز عبر أطواق الجهاز الإداري للبنتاغون. كان المحامي العام، على وجه الخصوص، في حاجة إلى الإقناع على نحو دامغ، بأن اختراق حواسيب عسكرية يعد أمرا مشروعا، حتى إن كان ذلك في إطار تدريب لاختبار أمنها. أشار محامو وكالة الأمن القومي إلى وثيقة تسمى توجيه الأمن القومي الرقم 42، كان الرئيس جورج دبليو بوش George H. W. Bush قد وقعها في العام 1990 (بوصفها تحديثا للتوجيه الرئاسي السري المتعلق بالأمن القومي «إن إس دي دي - 145» الذي أصدره ريغان)، وكانت الوثيقة تسمح صراحة بمثل هذه الاختبارات، إذا أعطى وزير الدفاع موافقة مكتوبة. وبالفعل، فقد وقع الوزير بيري على نموذج الاتفاق.

وضع المحامون قيدا واحدا فقط على التدريب، لم يكن ممكنا لمخترقي الحاسوب من وكالة الأمن القومي مهاجمة الشبكات الأمريكية باستخدام أي من معداتهم عالية السرية المستخدمة في استخبارات الإشارة (سيجينت)، فلم يكن باستطاعتهم استخدام معدات وبرمجيات سوى تلك المتاحة تجاريا.

في 16 فبراير من العام 1997[8]، أصدر الجنرال جون شاليكاشفيلي John Shalikashvili، رئيس الهيئة المشتركة لرؤساء الأركان، التعليمات الرقم 3510.01، وهي برنامج المناورات التدريبية للعمل المشترك من دون سابق إخطار، الذي كان يجيز سيناريو تدريب «المتلقِّي المؤهَّل»، ويتضمن وصفا له.

حدد التدريب سيناريو يتكون من ثلاث مراحل[9]. في المرحلة الأولى كان قراصنة حاسوب (هاكرز) ينتمون إلى كوريا الشمالية وإيران (أدى هذا الدور الفريق الأحمر لوكالة الأمن القومي) سيبدأون بهجوم منسق على البنى الأساسية الحرجة، وخاصة خطوط شبكات الكهرباء وخطوط اتصالات الطوارئ 911، في ثماني مدن أمريكية، هي: لوس أنجلوس Los Angeles، وشيكاغو Chicago، وديترويت Detroit، ونورفولك Norfolk، وسانت لويس St. Louis، وكولورادو سبرينغز Colorado Springs، وتامبا Tampa، وفايتيفيل Fayetteville، وجزيرة أواهو Oahu في هاواي Hawaii. (كانت هذه المرحلة تجرى كمناورة منضدية (نظريا بالمحاكاة)، مبنية على

تحليلات بشأن مدى سهولة تعطيل خطوط الشبكة وزيادة تحميل خطوط هاتف 911). وكما جاء في سيناريو المناورة، كان الهدف من الهجوم هو الضغط على القادة السياسيين الأمريكيين من أجل رفع العقوبات التي كانت أمريكا قد فرضتها أخيرا على كوريا وإيران.

في الجزء الثاني من المناورة، كان قراصنة حاسوب (الهاكرز) سيشنون هجوما هائلا واسع النطاق على الشبكات العسكرية الخاصة بالهاتف، والفاكس، والحاسوب؛ بداية في قيادة الولايات المتحدة في المحيط الهادي (الباسيفيك)، ثم في البنتاغون وغيره من منشآت وزارة الدفاع. كان الهدف المعلن هو عرقلة أنظمة القيادة والسيطرة في الولايات المتحدة، مما يجعل رؤية ومتابعة ما يجري أمرا عسيرا على الجنرالات، ويجعل رئيس الجمهورية يستجيب للتهديدات بالقوة. لم تكن هذه المرحلة ستتم بأسلوب المحاكاة، كان الفريق الأحمر في وكالة الأمن القومي سيَنْفُذ فعليا إلى الشبكات.

طوال ثلاثة أشهر ونصف الشهر، الفترة الفاصلة بين صدور تفويض رئيس الهيئة المشتركة لرؤساء الأركان والبداية الفعلية للمناورة، كان الفريق الأحمر بوكالة الأمن القومي يعد للهجوم، إذ تفحَّص الشبكات العسكرية والبروتوكولات المستخدمة فيها، وحدَّد الحواسيب التي ستُختَرَق، وكيفية اختراقها لإحداث أقصى تأثير.

كان الإعداد للمناورة وتنفيذها يجري في سرية تامة، وكان الجنرال شاليكاشفيلي قد أصدر أمر تدريب من دون سابق إخطار، ما كان يعني أنه لم يكن أحد يمكنه معرفة أن هناك تدريبا يجري، إلا من ينفذ ويرصد الهجوم؛ وحتى داخل وكالة الأمن القومي، لم يسمح لأحد بمعرفة هذا السر سوى كبار المسؤولين، والفريق الأحمر ذاته، ومحامي الوكالة، الذي كان يتعيَّن أن يعتمد كل خطوة يتخذها الفريق، ثم يبادر بإفادة كل من المستشار العام للبنتاغون والمدعي العام.

في إحدى المراحل في أثناء التدريب، تواصل توماس ماكديرموت Thomas McDermott - نائب مدير مديرية ضمان المعلومات بوكالة الأمن القومي، التي كانت تشرف على الفريق الأحمر - مع ريتشارد مارشالRichard Marshall - مستشار وكالة الأمن القومي – وأخبره بأنه قيد التحقيق بتهمة التجسس. كان أحد أفراد الأمن قد لاحظ أنه يأتي في أوقات غريبة، ويستخدم الهاتف الجوال المشفر على نحو أكثر من المعتاد.

سأل مارشال، بنبرة تحذيرية بعض الشيء: أنت تعرف لماذا أنا هنا، أليس كذلك؟
قال ماكديرموت: نعم، بالطبع، مطمئنا مارشال إلى أنه كان قد أطلع أحد ضباط الأمن على ما كان يحدث، وحتى ذلك الضابط كان قد تلقى تعليمات بألا يخبر زملاءه، لكن بدلا من ذلك يستمر في متابعة إجراءات التحقيق حتى إتمام المناورة.

كان تدريب «المتلقِّي المؤهَّل» الرقم 97 قد بدأ رسميا في يوم الإثنين 9 يونيو. وكان من المخطط أن يمتد التدريب أسبوعين، مع السماح بالتمديد أسبوعين آخرين إذا لزم الأمر. لكن المناورة انتهت مبكرا، إذ جرى النفاذ إلى شبكة مؤسسة الدفاع كلها في أربعة أيام. في اليوم الأول اخْتُرِق مركز القيادة العسكرية القومي، وهو المنشأة التي كانت ستنقل الأوامر من رئيس الولايات المتحدة في وقت الحرب، ولم يعرف معظم ضباط طاقم عمل هذه المخدمات أنهم كانوا قد تعرضوا للاختراق.

ثمة مجموعة واحدة فقط من الأهداف تجنبها الفريق الأحمر لوكالة الأمن القومي؛ بخلاف ذلك، ربما كانوا قد نجحوا في اختراقها، وهي الأربعة والعشرون مخدما حاسوبيا التابعة لسلاح الجو، والتي كان يرصدها محللو فريق استجابة الحاسوب في سان أنطونيو. اعتقد المخترقون أنهم كانوا سيُكْتَشفون إذا ما اخترقوا تلك الشبكات، فوجهوا هجماتهم لاستهداف أماكن أخرى، وتبين أن النفاذ إلى مواقع أخرى كان سهلا على نحو مضحك ومناف للعقل.

اتضح أن الكثير من حواسيب وزارة الدفاع لم تكن محمية بكلمة مرور، وحواسيب أخرى كانت محمية بكلمات مرور عرجاء وضعيفة، مثل: كلمة مرور password، أو أيه بي سي دي إي ABCDE، أو 12345. في بعض الحالات كان الفريق الأحمر يقطع كل وصلات اتصالات المكتب باستثناء خط الفاكس، ثم يغمر ذلك الخط باتصال تلو الآخر، حتى يُوقَف تشغيله. في حالات قليلة، كان ملحقا وكالة الأمن القومي - أحدهما داخل البنتاغون، والآخر في منشأة في هاواي تابعة لقيادة المحيط الهادي – يذهبان لنبش مكب النفايات وسلال المهملات، بحثا عن كلمات المرور. هذه الحيلة أيضا آتت ثمارها.

كان أصعب وقت على الفريق هو حينما حاول اختراق المخدم الحاسوبي الخاص بمديرية استخبارات هيئة الأركان المشتركة (جيه2- J-2). في نهاية المطاف، ببساطة اتصل أحد أعضاء الفريق بمكتب المديرية، وأخبرهم بأنه من قسم تكنولوجيا

المعلومات في البنتاغون، وأن هناك بعض المشكلات التقنية، وهو في حاجة إلى إعادة ضبط واسترجاع كل كلمات المرور، ولم يتردد الشخص الذي رد على الهاتف[10]، وأعطاه كلمة المرور الحالية. واقتحم الفريق الأحمر.

في معظم الأنظمة التي نفذوا إليها، ترك عناصر الفريق الأحمر علامة، هي المكافئ الرقمي لعبارة كيلروي كان هنا Kilroy was here(*). في بعض الحالات فعلوا أكثر من ذلك بكثير، مثل: اعتراض الاتصالات وتحويرها، وإرسال رسائل بريد إلكتروني مزيفة، وحذف ملفات، وإعادة تهيئة محركات الأقراص الصلبة. كان كبار الضباط ممن لم يكن لديهم علم بشأن التدريب يجدون خطوط الهاتف ميتة لا تعمل، ورسائل أُرسلت لكن لم تُتَسلَّم (أو أرسلت، لكنها تبلغ شيئا مختلفا تماما عند وصولها)، وأنظمة بأسرها توقفت عن التشغيل أو كانت تنفث هراء من بيانات لا معنى لها. أرسل أحد الضباط الذين تعرضوا لهذا الوابل إلى قائده رسالة بريد إلكتروني (اعترضها الفريق الأحمر)، قائلا: أنا لا أثق بنظام القيادة والسيطرة الذي لديَّ.

كان هذا هو الهدف الأساسي من وسائل حرب المعلومات، وكشف تدريب «المتلقِّي المؤهَّل» أن الأمر كان ذا جدوى أكثر مما كان أي شخص في عالم وسائل الحرب التقليدية قد تخيل.

بعد بضعة أسابيع من انتهاء التدريب أعد ضابط في سلاح الجو برتبة بريجادير جنرال (عميد) يدعى جون سوب كامبل John Soup Campbell تقريرا موجزا لتقييم الموقف بشأن التدريب، كان كامبل طيارا مقاتلا على الطائرات طراز إف-15، ولم يكن قد نُقل إلى البنتاغون إلا حينما كان تدريب «المتلقِّي المؤهَّل» قد بدأ بالفعل. كانت مهمته الجديدة هي رئاسة جيه39- (J-39)، وهو مكتب داخل مديرية العمليات في هيئة الأركان المشتركة، كان بمنزلة حلقة الوصل بين مديري برامج الأسلحة فائقة السرية والقادة العسكريين الميدانيين. كانت هيئة الأركان المشتركة في حاجة إلى شخص ليكون رجلها المسؤول في تدريب «المتلقِّي المؤهَّل»، وحصل كامبل على المهمة.

(*) كيلروي كان هنا Kilroy was here، هو تعبير أمريكي أصبح شائعا خلال الحرب العالمية الثانية، وعادة ما يشاهد في الرسوم على الجدران مصحوبا برسم لرجل ذي رأس أصلع مع أنف بارز يطل على جدار وأصابعه تمسك الجدار. أصبحت العبارة والرسم المميز مرتبطين بالجنود في الأربعينيات. [المترجم].

قدم كامبل تقريره الموجز إلى مجموعة صغيرة كانت تضم مسؤولين مدنيين رفيعي المستوى، ونواب قادة الأركان في سلاح الجو، وسلاح البحرية ـ ومشاة البحرية. كان الجيش الميداني (القوات البرية) قد قرر عدم المشاركة في التدريب، إذ إن بضعة من ضباطه أدركوا أن لديهم ثغرات، وأن قواتهم غير محصنة، ورغبوا في أن يتفادوا تعرضهم للإحراج. كان معظمهم قد رفض الموضوع على أنه مضيعة للوقت.

كانت رسالة كامبل جلية وصارخة. كشف تدريب «المتلقِّي المؤهَّل» أن وزارة الدفاع غير مستعدة نهائيا، وعاجزة عن صد هجوم سيبراني. كان الفريق الأحمر بوكالة الأمن القومي قد تغلغل إلى شبكتها بأسرها. لم يكن أحد قد أدرك أن هناك هجوما يجري سوى بضعة ضباط فقط، ولم يكن أي منهم على دراية بما يجب فعله حيال ذلك، لم تكن قد صدرت مطلقا أي مبادئ توجيهية أو إرشادات، ولم تُعَدّ أي سلسلة أوامر. شخص واحد فقط في وزارة الدفاع بكاملها هو الذي صد الهجوم بطريقة فعالة، وهو ضابط تقني في إحدى وحدات مشاة البحرية في المحيط الهادئ (الباسيفيك)، حيث رأى أن شيئا غريبا شاذا يحدث للمخدم الحاسوبي، فعمد إلى فصله خارج الشبكة بمبادرة شخصية منه.

بعد الإحاطة التي قدمها كامبل، قدم رئيس الفريق الأحمر لوكالة الأمن القومي، وهو ضابط في سلاح البحرية برتبة كابتن (نقيب) يدعى مايكل سير Michael Sare، عرضا. وتحسبا لتشكك أي شخص في ادعاءاته، أحضر كامبل معه سجلات الاقتحام، متضمنة صورا لقوائم كلمات المرور التي استرجعوها من مكبات النفايات، وتسجيلات صوتية لمحادثات هاتفية يبوح فيها الضباط بكلمات السر للغرباء بإهمال ومن دون مبالاة، وأكثر من ذلك بكثير. (كان سير في المسودة الأصلية لتقريره قد أشار إلى أن الفريق كسر كلمة المرور الخاصة برئيس الهيئة المشتركة لرؤساء الأركان، وكان مينيهان قد قرأ المسودة مسبقا، وطلب من سير أن يمحو ذلك السطر. فسَّر مينيهان ذلك بأنه لا حاجة إلى إثارة غضب جنرال من فئة النجوم الأربعة).

كان الجميع في الغرفة مذهولين، لاسيما جون هامري John Hamre، الذي كان في نهاية شهر يوليو قد أدى اليمين الدستورية بوصفه نائبا لوزير الدفاع. قبل ذلك الوقت، كان هامري هو المراقب المالي للبنتاغون، حيث كان قد خاض حربا من أجل خفض الموازنة العسكرية، وبخاصة الجزء السري المخصص لوكالة الأمن القومي.

خلال الثمانينيات من القرن العشرين، وبوصفه عضوا في هيئة مكتب الموازنة في الكونغرس، وعضوا في لجنة الخدمات (الفروع) المسلحة في مجلس الشيوخ، كان هامري قد نشأ على عدم الثقة بوكالة الأمن القومي. لقد كانت جماعة مراوغة، سرية جدا، تسبح في المنطقة الرمادية بين العسكرية والاستخبارات، وتتملص من القيود التي على كلتيهما. لم يكن هامري يعرف أي شيء بشأن وسائل حرب المعلومات، ولم يكن يهتم.

قبل بضعة أسابيع من تدريب «المتلقِّي المؤهَّل»، بينما كان يجري إعداد هامري لترقيته، كان مينيهان قد أطلعه على ما لوسائل حرب المعلومات من تهديدات وفرص، وعلى الحاجة إلى موازنة أكبر من أجل استغلال الفرص ودرء التهديدات. تنهَّد هامري مصدوما بالتفاصيل التقنية، وقال: كين، أنت تصيبني بالصداع.

لكن طرأ تحوُّل على هامري وهو يستمع إلى كامبل وسير بينما كانا يستعرضان نتائج تدريب «المتلقِّي المؤهَّل»، استولى عليه الشعور بالضرورة الملحة. جال ببصره في أرجاء الغرفة المملوءة بالجنرالات والضباط برتبة الكولونيل (العقيد)، وسأل: من الذي كان مسؤولا عن إصلاح هذه المشكلة؟

نظر الجميع إليه ثانية. لم يكن أحد يعرف الإجابة. لم يكن أحد مسؤولا.

في الوقت نفسه تقريبا، كان كين مينيهان يقدم إحاطته حول تدريب «المتلقِّي المؤهَّل» إلى لجنة مارش. في تلك الأثناء كانت اللجنة قد غاصت بعمق في الحالة الهشة للبنية الأساسية الحرجة. لكن السيناريوهات التي درستها كانت افتراضية (نظرية) وكانت تتناول أوجه الضعف والثغرات الأمنية للقطاعات المدنية (غير العسكرية)، إذ لم يكن أحد قد شن هجوما سيبرانيا فعليا، وكان معظم أعضاء اللجنة قد افترض أن شبكات الجيش آمنة. حطمت إحاطة مينيهان أوهامهم في كلا الأمرين، لقد شن الفريق الأحمر لوكالة الأمن القومي هجوما فعليا، وكانت آثاره مدمرة.

واقعة واحدة في تدريب «المتلقِّي المؤهَّل» هي التي لم يكشف عنها مينيهان، واقعة لم يعرف بها سوى بضعة مسؤولين. حينما اخترق أعضاء الفريق الأحمر الشبكات باعتبار ذلك جزءا من التدريب، صادفوا بعض غرباء يمكن عزوهم إلى عناوين إنترنت فرنسية، كانوا يخترقون الشبكة فعليا. بعبارة أخرى، كان هناك جواسيس أجانب ينفذون بالفعل إلى الشبكات الحيوية غير الحصينة. لم يكن الخطر افتراضيا.

حتى من دون هذه الرواية، كان أعضاء اللجنة مصدومين. سأل مارش: ما الذي كان يمكن عمله لإصلاح المشكلة. أجاب مينيهان: غيروا القانون، امنحوني السلطة، أنا سأحمي الأمة.

لم يكن أحد يعرف تماما ما الذي كان يعنيه؛ أو إذا كان يقصد ما اعتقدوا أنه كان يقصده، لم يأخذه أحد على محمل الجد، لم يكن أحد سيعيد إحياء التوجيه الرئاسي السري المتعلق بالأمن القومي (إن إس دي دي-145) الذي كان ريغان قد أصدره، أو ينعش أي شيء من هذا القبيل.

في 13 أكتوبر، نشرت لجنة مارش تقريرها بعنوان ركائز حاسمة Critical Foundations، ولم يقدم سوى لمحة موجزة[11] عن مناورة تدريب «المتلقِّي المؤهَّل». على نحو رئيسي، ركزت التوصيات الواردة في التقرير على حاجة الحكومة والقطاع الخاص إلى تشارك المعلومات، وحل المشكلات معا. لم يذكر التقرير شيئا بشأن منح وكالة الأمن القومي المزيد من المال أو السلطة.

بعد مضي أربعة أشهر، وقع هجوم آخر على شبكات وزارة الدفاع، هجوم بدا مشابها لتدريب «المتلقِّي المؤهَّل»، لكنه جاء من قراصنة حاسوب (هاكرز) حقيقيين مجهولين في العالم الخارجي الحقيقي.

5

هجمات «الشروق الشمسي» و«متاهة ضوء القمر»

«كانت هناك أزمة دولية تختمر، وربما تكون الحرب في الأفق؛ لذا كان من الطبيعي افتراض الأسوأ»

في 3 فبراير 1998[1] انطلقت صافرات الإنذار من أجهزة مراقبة الشبكة في مركز سلاح الجو لوسائل حرب المعلومات في سان أنطونيو، كان شخص ما يخترق حاسوب الحرس الوطني في قاعدة «أندروز» الجوية بأطراف واشنطن العاصمة.

في غضون أربع وعشرين ساعة، ومن خلال تقصي الشبكات بمزيد من التعمق، اكتشف فريق المركز للاستجابة لطوارئ الحاسوب حدوث تسلل في ثلاث قواعد أخرى. وبتتبع تحركات مخترق الحاسوب وجد الفريق أنه كان قد اقتحم الشبكة عبر مخدم حاسوبي يتبع معهد ماساتشوستس للتكنولوجيا. حالما صار المخترِق داخل المواقع العسكرية، نَصَّب «متلصص حزم»

(مراقب شبكة) packet sniffer[*]، جمع أدلة أسماء المستخدمين وكلمات المرور، مما أتاح له التجوال في الشبكة بأسرها. بعد ذلك أنشأ مختَرِق الحاسوب بابا خلفيا مكّنه من الدخول والخروج من الموقع كيفما يحلو له، وتنزيل، أو محو، أو تشويه أي بيانات كيفما شاء.

استطاع مخترق الحاسوب القيام بكل ذلك بسبب وجود ثغرة أمنية معروفة جيدا في نظام التشغيل «يونيكس» UNIX المستخدم على نطاق واسع. لقد كان اختصاصيو الحاسوب في سان أنطونيو يحذرون كبار الضباط من هذه الثغرة الأمنية، وكان كين مينيهان قد حذر الجنرالات في البنتاغون من تلك الثغرة الأمنية مرارا وتكرارا، لكن لم يأبه أحد.

في يوليو 1996، حينما وقَّع الرئيس كلينتون على الأمر التنفيذي بشأن «حماية البنية الأساسية الحرجة»، كان أحد تداعيات الأمر التنفيذي تشكيل لجنة «مارش». لكن كانت هناك نتيجة أخرى أقل وضوحا في ذلك الوقت، هي إنشاء فريق عمل حماية البنية الأساسية داخل وزارة العدل، ليضم عناصر من مكتب التحقيقات الفدرالي، والبنتاغون (هيئة الأركان المشتركة ووكالة نظم معلومات الدفاع)، وبالطبع وكالة الأمن القومي.

بحلول 6 فبراير، بعد ثلاثة أيام من رصد عملية التسلل في قاعدة «أندروز» الجوية، تولى ذلك الفريق القضية، والتعامل مع الأدلة الجنائية الحاسوبية بواسطة محللين من وكالة الأمن القومي، ووكالة نظم معلومات الدفاع، ووحدة في هيئة الأركان المشتركة تسمى «خلية الاستجابة للعمليات المعلوماتية»، أنشئت قبل ذلك بأسبوع واحد على أثر تدريب «المتلقِّي المؤهَّل». اكتشف فريق العمل أن المخترق استغل ثغرة أمنية محددة في أنظمة «يونيكس» المعروفة باسم «الشروق الشمسي 2.4 و2.6 Sun Solaris 2.4 and 2.6». لذلك، أطلق فريق العمل على تحقيقاتهم «الشروق الشمسي» اسما رمزيا لها.

(*) متلصص الحزم أو محلل الحزمة packet sniffer، هو برنامج حاسوبي أو جهاز يمكنه اعتراض حركة البيانات التي تمر عبر شبكة رقمية وتسجيلها، وتسمى هذه العملية «التقاط الحزم». مع تدفق تيار البيانات عبر الشبكة، يلتقط محلل الحزمة كل حزمة، وإذا لزم الأمر، يفكّ شفرة البيانات الأولية للحزمة، ويُظهر قيم حقولها المختلفة، ويحلل محتواها وفقا لمواصفات قياسية محددة. [المترجم].

كان جون هامري، نائب وزير الدفاع، قد رأى تدريب «المتلقّي المؤهَّل» قبل ذلك بثمانية أشهر على أنه ناقوس خطر للتنبيه إلى نوع جديد من التهديد. وحاليا، كان يرى أن عملية «الشروق الشمسي» هي تنفيذ لذلك التهديد. وفي إحاطته التي قدمها إلى الرئيس كلينتون بشأن ما حدث من تسلل، حذر هامري من أن «الشروق الشمسي» ربما يكون «أولى طلقات[2] حرب سيبرانية حقيقية»، مضيفا أنها ربما تكون قد أُطلقت بواسطة العراق.

لم يكن اشتباها أحمق غير مدروس. كان صدام حسين في الآونة الأخيرة قد طرد مفتشي الأمم المتحدة الذين بقُوا في العراق طوال ستة أعوام لضمان التزامه بشروط السلام التي أنهت عملية «عاصفة الصحراء»، لاسيما البند الذي كان يمنعه من تطوير أسلحة الدمار الشامل. تخوف كثيرون من أن يكون طرد صدام المفتشين هو مقدمة ليستأنف برنامج أسلحة الدمار الشامل لديه. كان كلينتون قد أمر جنرالاته بالتخطيط لاتخاذ إجراء عسكري، وأبحرت حاملة طائرات أخرى نحو الخليج العربي. كانت القوات الأمريكية تستعد لانتشار محتمل.

لذلك، حينما امتد اختراق «الشروق الشمسي» إلى أكثر من 12 قاعدة عسكرية، فإن البعض، لاسيما داخل هيئة الأركان المشتركة، استوقفتهم غرابة نمط حدوث الأمر. استهدف الاختراق قواعد في تشارلستون Charleston، ونورفولك Norfolk، ودوفر Dover، وهاواي Hawaii، وجميعها مراكز رئيسية لنشر القوات المسلحة الأمريكية. لم يُخْترق سوى المخدمات غير السرية، لكن بعض عناصر الدعم العسكري الحيوية، مثل: النقل، واللوجيستيات، والفرق الطبية، ونظام تمويل الدفاع؛ كان تشغيلها يجري على شبكات غير سرية. إذا أتلف مخترق الحاسوب (الهاكر) هذه الشبكات أو أوقف تشغيلها، فإنه كان سيمكنه أن يعوق، وربما يحول دون، رد فعل عسكري أمريكي.

بعد ذلك، جاء تقرير آخر مثير للقلق. كان محللو الأدلة الجنائية الحاسوبية في وكالة الأمن القومي ووكالة نظم معلومات الدفاع يتعقبون مسار مخترق الحاسوب، وهذا قادهم إلى عنوان على «إمارنت» Emirnet، وهو مزود خدمة إنترنت في دولة الإمارات العربية المتحدة، مما عزز المخاوف من أنه ربما يكون صدام، أو أي مفوض في المنطقة، وراء الهجمات.

أرسل مدير الاستخبارات القومية بمكتب التحقيقات الفدرالي برقية إلى جميع عملائه الميدانيين، مشيرا إلى «قلق من أن التسلل[3] ربما تكون له صلة بالأعمال العسكرية الأمريكية الجارية حاليا في الخليج العربي». أما في «فورت ميد»، فكان كين مينيهان أكثر حزما، إذ أخبر مساعديه بأنه يبدو أن مخترق الحاسوب (الهاكر) هو «كيان شرق أوسطي».

ارتاب البعض. حينما فوجئ الجميع بهجوم «الشروق الشمسي» الحقيقي، فإن نيل بولارد Neal Pollard، وهو استشاري شاب في وكالة نظم معلومات الدفاع، وكان قد درس علم التشفير والعلاقات الدولية، كان يخطط لمناورة تدريبية استكمالا لتدريب «المتلقِّي المؤهَّل». ومع انتشار حوادث التسلل، نزَّل بولارد السجلات logs من الحاسوب، ودوَّن ملخصات لجلسات الإحاطة، في محاولة لفهم نيات مخترِق الحاسوب (الهاكر). كان كلما فحص مزيدا من البيانات، ازداد ارتيابه أن ذلك كان من عمل أشرار خطرين.

كان بولارد يخطط لتدريب ينْفُذ من خلاله الفريق الأحمر إلى شبكة عسكرية غير سرية، ومنها يبحث عن سبيل إلى شبكتها السرية (التي كان بولارد يعرف من تقص مسبق، أنها لم تكن آمنة تماما)، ويقفز إليها، ويقتحمها. على النقيض من ذلك، لم يكن مخترق الحاسوب في «الشروق الشمسي» يفعل من بُعد أي شيء يتسم بالإحكام، كان هذا الرجل يتجول فترة وجيزة في الأنظمة غير السرية الواحد تلو الآخر، ثم يخرج، لم يخلف وراءه أي برمجيات ضارة، ولا أبوابا خلفية، لا شيء. وبينما كانت بعض المخدمات التي هاجمها هي على وجه الدقة حيث كان سيذهب أي مخترق حاسوب لتقويض شبكة جيش على وشك الانتشار، فإن معظم الأهداف بدا أنها اخْتيرت على نحو عشوائي، من دون أن تكون لها دلالة البتة.

مع ذلك، كانت هناك أزمة دولية تختمر، وربما تكون الحرب في الأفق؛ لذا كان من الطبيعي افتراض الأسوأ. أيا ما كانت هوية المخترق أو دوافعه، فإنه كان يسعى إلى أن يفقد القادة توازنهم. هم تذكروا تدريب «المتلقِّي المؤهَّل»، حينما لم يدرك أحد أنهم كانوا قد تعرضوا للاختراق، كان الفريق الأحمر لوكالة الأمن القومي قد دس لهم بعض الرسائل الزائفة، وهم افترضوا أنها حقيقية. في هذه المرة، عرفوا أنهم يتعرضون للاختراق، وأن الأمر لم يكن مناورة تدريبية. إنهم لم يكتشفوا أي ضرر أو

عطب، لكن كيف كان يمكنهم التأكد من ذلك؟ حينما كانوا يقرأون إحدى الرسائل أو ينظرون إلى إحدى الشاشات، هل كان من الممكن أن يثقوا بما كانوا يرونه؟ وهل كان ينبغي عليهم الوثوق بما كانوا يرونه؟

كان هذا هو الأثر المنشود لما كان بيري قد أسماه وسائل الحرب المضادة للقيادة والسيطرة. إن مجرد معرفة أنك قد تعرضت للاختراق، بغض النظر عن آثاره الملموسة، يكون أمرا مربكا ومزعزعا.

في تلك الأثناء، كان فريق عمل وزارة العدل يتعقب مخترق الحاسوب (الهاكر) على مدار اليوم. كان إجراء شاقا مضنيا. كان مخترق الحاسوب يقفز من خادم إلى آخر لإخفاء هويته ومصدره؛ كان على وكالة الأمن القومي إبلاغ مكتب التحقيقات الفدرالي بشأن كل تلك القفزات، وكان بدوره يستغرق يوما أو نحو ذلك للتحقيق في كل تقرير. عند هذه النقطة لم يكن أحد يعرف ما إذا كان إمارنت، مزود خدمة الإنترنت في الإمارات العربية المتحدة، هو مصدر الهجمات أو أنه مجرد نقطة واحدة من عدة نقاط هبوط على امتداد قفزات المخترق.

لاحظ بعض محللي خلية الاستجابة للعمليات المعلوماتية، الوحدة حديثة الإنشاء في هيئة الأركان المشتركة، أن هناك نسقا واحدا في عمليات الاقتحام، فجميعها حدث فيما بين الساعة السادسة والساعة الحادية عشرة مساء بتوقيت الساحل الشرقي الأمريكي. حسب المحللون الساعة حيثما كان يعمل المخترق. تبين أنه ربما كان في مناوبة ليلية في بغداد أو في موسكو، أو ربما كان في مناوبة الصباح الباكر في بكين.

أحد الاحتمالات الذي لم يكلفوا أنفسهم عناء التفكير فيه، هو أنه كان أيضا وقت ما بعد انتهاء الدوام المدرسي في ولاية كاليفورنيا California.

بحلول يوم 10 فبراير، بعد أربعة أيام من التقصي، اكتشف فريق العمل الجناة مرتكبي الحادث. إنهم لم يكونوا عراقيين أو «كيانات شرق أوسطية» بأي عشيرة أو جنسية. كانا صبيين في عمر السادسة عشرة في ضواحي سان فرانسيسكو San Francisco، نسل شرير ومخرِّب للشخصية التي جسدها ماثيو برودريك في فيلم «ألعاب الحرب» (المناورات الحربية)، يخترقان شبكة الإنترنت تحت أسماء مستخدمين، هي: ماكافيلي Makaveli وستيمبي Stimpy، وكانا يتنافسان مع أصدقائهما على من هو الأسرع في اختراق البنتاغون.

في يوم واحد، حصل عملاء مكتب التحقيقات الفدرالي على تصريح بالتنصت من أحد قضاة المحكمة، وأخذوا التصريح إلى «سونيك.نت» Sonic.net، مزود الخدمة الذي كان يستخدمه الصبيان، وبدأوا في تعقب كل ضغطة زر يُجريها الصبيان، بدءا من لحظة تسجيل الدخول عبر خط الهاتف الخاص بوالدي ستيمبي. أكدت فرق المراقبة المادية (الجسدية) أن الولدين كانا في المنزل، كان هذا دليل شاهد عيان (دليلا عيانيا) على تورطهما، في حالة ما إذا ادعى محامي الدفاع لاحقا براءة الصبيين، وأنه لا لوم عليهما، وأنه لا بد أن شخصا آخر قد اخترق المخدم الحاسوبي الخاص بهما.

من خلال التنصت، علم العملاء أن الصبيين كانا يحصلان على مساعدة من فتى إسرائيلي يبلغ من العمر ثمانية عشر عاما، وهو بالفعل مخترق حاسوب (هاكر) سيئ السمعة يدعى إيهود تينينباوم Ehud Tenenbaum، ويطلق على نفسه اسم «المحلل» The Analyzer. كان المراهقون الثلاثة وقحين وحمقى. كان «المحلل» شديد الثقة بمهارته، إلى حد أنه قدم عرضا حيا لاختراقه شبكة عسكرية في أثناء مقابلة أجراها مع منتدى عبر الإنترنت يسمى «أنتي أونلاين» AntiOnline، الذي كان مكتب التحقيقات الفدرالي يرصده. أيضا، أعلن أنه كان يضطلع بتدريب الصبيين في كاليفورنيا لأنه كان «مقدما على التقاعد»[4] وكان في حاجة إلى خلفاء. كذلك أجرى ماكافيلي مقابلة أوضح فيها دوافعه الخاصة، إذ كتب «إنه النفوذ، يا صاح. أنت تعرف، النفوذ».

كان من المقرر أن يدع فريق عمل وزارة العدل الصبيين فترة أطول قليلا لإحكام الخناق عليهما. لكن في يوم 25 فبراير تحدث جون هامري إلى مراسلي الصحف في مأدبة إفطار صحافية في واشنطن العاصمة. كان لايزال محبطا من تقاعس الجيش تجاه التهديد السيبراني الأوسع نطاقا، وعرض بإيجاز الحقائق الأساسية بشأن «الشروق الشمسي» - الذي كان سريا حتى ذلك الحين - واصفا إياه بأنه حتى تاريخه هو «الهجوم الممنهج الأكثر تنظيما»[5] على أنظمة الدفاع الأمريكية، وكشف عن أن المشتبه فيهما كانا اثنين من المراهقين في كاليفورنيا الشمالية Northern California.

عند هذه النقطة، كان على مكتب التحقيقات الفدرالي أن ينطلق على الفور قبل أن يسمع الصبيان بشأن تصريحات «هامري» ويمحوا ملفاتهما، وسرعان ما حصل

العملاء على إذن تفتيش ودخلوا إلى منزل ستيمبي. كان ستيمبي موجودا في غرفة نومه، جالسا أمام جهاز الحاسوب، محاطا بعلب المشروبات الغازية الفارغة، وبقايا شطائر لحم بالجبن (تشيزبرغر). اعتقل العملاء الصبيين، وتحفظوا على الحاسوب والعديد من الأقراص المرنة.

حُكم على ستيمبي وماكافيلي (اللذين لم يعلن اسماهما الحقيقيان لكونهما حدثين) بالسجن ثلاثة أعوام بإفراج مشروط ومائة ساعة من الخدمة المجتمعية، ومُنعا من الولوج إلى الإنترنت من دون إشراف من الكبار. أما تيننباوم فقد ألقت الشرطة الإسرائيلية القبض عليه[6] هو وأربعة من تلاميذه، الذين كانوا جميعا في العشرين من العمر؛ وأمضى في السجن ثمانية أشهر، بعدها أسس شركة لأمن المعلومات، ثم انتقل إلى كندا، حيث أُلقي القبض عليه بتهمة اختراق مواقع مالية وسرقة أرقام بطاقات ائتمان.

في البداية، شعر بعض مسؤولي الولايات المتحدة الرسميين بالارتياح لأن قراصنة الحاسوب (الهاكرز) في هجوم «الشروق الشمسي» لم يكونوا إلا اثنين من الصبية؛ أو كما ذكر أحد مسؤولي مكتب التحقيقات الفدرالي في إحدى المذكرات: «لا يزيد على كونه أحد الاختراقات المعتادة[7] المنتشرة هذه الأيام». لكن معظم المسؤولين أخذوا ذلك على أنه يدعو إلى عدم الاطمئنان، إذا استطاع طفلان فعل هذا، فما الذي كان سيمكن أن تفعله دولة قومية معادية ممولة تمويلا جيدا؟

إنهم كانوا على وشك معرفة ذلك.

في أوائل شهر مارس، بينما كان المسؤولون في وكالة الأمن القومي، ووكالة نظم معلومات الدفاع، وخلية الاستجابة للعمليات المعلوماتية بهيئة الأركان المشتركة؛ يغلقون ملفاتهم الخاصة بقضية «الشروق الشمسي» والعودة إلى مهامهم الاعتيادية، وصلت إخبارية بأن شخصا اخترق الحواسيب في قاعدة «رايت-باترسون» الجوية بولاية أوهايو Ohio، وكان يسرق ملفات - غير سرية لكنها حساسة - بشأن تصميم مقصورة قيادة ومخططات لرقائق إلكترونية دقيقة.

على مدى الأشهر القليلة اللاحقة، انتشر مخترق الحاسوب (الهاكر) إلى منشآت عسكرية أخرى. لم يكن أحد يعرف مكانه، كانت قفزاته من موقع إلى آخر محيرة، وخاطفة، وعمومية شاملة. لم تكن عمليات البحث التي أجراها تحمل أي نسق

واضح، عدا أنها كانت تتضمن مشروعات بحث وتطوير عسكرية رفيعة المستوى. كانت العملية نوعا ما تتمة لهجوم «الشروق الشمسي»، على رغم أنها كانت على نطاق أوسع ومحيرة أكثر. لذا، وتماما مثلما يعقب الليل النهار، أطلق فريق العمل عليها اسم عملية «متاهة ضوء القمر» Moonlight Maze.

مثل عصابة هجوم «الشروق الشمسي»، كان مخترق الحاسوب هذا يسجل دخوله للولوج إلى حواسيب مختبرات الأبحاث الجامعية ليحصل منها على إمكانية الوصول إلى مواقع وشبكات عسكرية. لكن من جهة أخرى فإنه لم يكن مطلقا يبدو مثل طفل عابث مخرب، مولع بالإزعاج والأذى، يقوم بنزهة سيبرانية. إنه لم يكن يندفع واثبا من أحد المواقع وإليه، كان مثابرا يبحث عن معلومات محددة، وبدا أنه كان يعرف أين يجدها، وإذا لم يفضِ مساره الأول إلى شيء، كان يبقى داخل الشبكة، ويجوبها باحثا عن منافذ أخرى.

كان أيضا متمرسا على نحو لافت، ويستخدم أساليب بهرت حتى فرق وكالة الأمن القومي التي كانت تتعقب تحركاته. كان يسجل دخوله إلى أحد المواقع مستعينا باسم مستخدم وكلمة مرور مسروقين؛ وحينما كان يغادر، كان يعيد كتابة ملف تسجيل أحداث الحاسوب the log file حتى لا يتمكن أحد من معرفة أنه كان هناك من قبل. كان مخترق الحاسوب (الهاكر) جد خطير، لذا كان لزاما على المحللين الإمساك به متلبسا بالجرم المشهود، وتتبع تحركاته آنيا في الوقت الحقيقي؛ ولأنه كان يمحو السجلات عند خروجه، فإن الأدلة التي كانت تظهر على الشاشة حتى ذلك الحين كانت ستختفي بعد الواقعة. لقد استغرق الأمر بعض الوقت والجهد لإقناع بعض كبار المسؤولين بحدوث تسلل.

قبل ذلك بعام، على الأرجح لم يكن المحللون ليكتشفوا أي مخترق حاسوب مطلقا إلا بمحض المصادفة. كان ما يقرب من ربع مخدمات سلاح الجو متصلة براصدات أمن الشبكات في سان أنطونيو؛ لكن معظم قادة الجيش الميداني (القوات البرية)، وسلاح البحرية، والمدنيين (غير العسكريين) في البنتاغون لم تكن لديهم أي وسيلة لمعرفة ما إذا كان هناك متسلل، فضلا عن معرفة ما الذي كان يفعله أو من أين أتى.

لقد تغير كل ذلك مع اللكمات القاضية المتمثلة في تدريب «المتلقِّي المؤهَّل»، وتقرير لجنة «مارش»، وتحقيقات «الشروق الشمسي»، التي أدت في غضون ثمانية

أشهر فقط، من يونيو من العام 1997 حتى فبراير من العام 1998، إلى إقناع كبار المسؤولين، حتى أولئك الذين لم يكن قد سبق لهم مطلقا التفكير في شأن المسألة، أقنعتهم أن أمريكا كانت عرضة لهجوم سيبراني، وأن هذه الحالة لا تهدد البنية الأساسية للمجتمع فقط، بل تهدد أيضا قدرة الجيش على التحرك في حالة الأزمة.

عقب تدريب «المتلقِّي المؤهَّل» مباشرة، دعا جون هامري إلى اجتماع يضم كبار المدنيين وكبار ضباط البنتاغون لبحث ما الذي كان سيمكن عمله. أحد الحلول السهلة نسبيا لسد الثغرات، كان هو السماح بشراء طارئ لأجهزة تعرف باسم «أنظمة كشف التسلل» intrusion-detection systems (IDS)، وتركيبها على أكثر من مائة حاسوب في وزارة الدفاع. إحدى الشركات في مدينة أتلانتا Atlanta بولاية جورجيا Georgia تسمى «أنظمة أمن الإنترنت»، كان سيمكنها تصنيع تلك الأجهزة بكميات كبيرة. نتيجة لذلك، حينما اندلعت هجمات «الشروق الشمسي» وعملية «متاهة ضوء القمر»، فإن عددا كبيرا من موظفي البنتاغون رأوا ما كان يجري أنه أسرع كثيرا مما تعودوه.

لم يكن الجميع قد فهم الرسالة. عقب تدريب «المتلقِّي المؤهَّل»، فإن مات ديفوست Matt Devost، الذي كان قد قاد الفريق المهاجم في تدريب فحص أوجه الضعف والثغرات الأمنية في أنظمة القيادة والسيطرة الأمريكية والحليفة، أُوفِد إلى هاواي لتطهير الشبكات في مقر قيادة الولايات المتحدة في المحيط الهادئ (الباسيفيك)، التي كان الفريق الأحمر بوكالة الأمن القومي قد اجتاحها. وجد ديفوست ثغرات وتخاذلا في كل مكان. كان مصنعو البرمجيات قد أصدروا منذ فترة طويلة تحذيرات بشأن الثغرات الأمنية في برمجياتهم، مع برامج تصحيح لإصلاحها؛ وببساطة، كان على مستخدم البرمجية الضغط على زر. في العديد من الحالات، وجد ديفوست أنه حتى هذا لم يكن أحد قد نفذه في مقر قيادة المحيط الهادئ (الباسيفيك). ألقى ديفوست محاضرة على الأدميرالات، وكان جميعهم في سن أكثر من ضعف عمره. قال ديفوست إن هذا لم يكن أمرا معقدا مثل علم الصواريخ. لم يكن الأمر يتطلب سوى وضع أحد في محل المسؤولية، وأمره بتنصيب الإصلاحات. حينما اندلع اعتداء «الشروق الشمسي»، كان ديفوست يعمل في مجال الأدلة الجنائية الحاسوبية في وكالة نظم معلومات الدفاع، وصادف أنه اطلع على

سجلات logs قيادة المحيط الهادئ (الباسيفيك)، ورأى أنهم لم يصلحوا ما لديهم من مشكلات، وعلى الرغم من جهوده المضنية، لم يكن أي شيء قد تغير (عند هذه النقطة، قرر ديفوست ترك الحكومة والعمل في القطاع الخاص في مجال نماذج محاكاة الاعتداء الحاسوبي).

حتى بعض الضباط الذين كانوا قد أجروا التغييرات، ونصبوا الأدوات، لم يكن أحد منهم يفهم ما الذي كان يفعله. بعد ستة أشهر من صدور الأمر بوضع أنظمة كشف التسلل على حواسيب وزارة الدفاع - قبل «الشروق الشمسي» بأسابيع قليلة - دعا هامري إلى اجتماع ليتبيَّن حالة عمل الأجهزة.

قَطَّب جنرال ذو نجمة واحدة من الجيش الميداني (القوات البرية) جبينه، وتذمر من أنه لم يكن يعرف بشأن تلك الأنظمة التي تسمى «أنظمة كشف التسلل»، فمنذ أن وضعها على حواسيبه، كانوا يتعرضون للهجوم يوميا. حبس الآخرون على الطاولة ضحكاتهم. لم يكن الجنرال يُدرك أن حواسيبه ربما كانت تتعرض للقرصنة على نحو يومي طوال أشهر وربما طوال أعوام. كل ما فعلته أنظمة كشف التسلل هو أنها جعلته يعلم بذلك عند حدوثه.

في بدايات هجوم «الشروق الشمسي»، دعا هامري إلى اجتماع آخر، مشبعا بقلق الشعور بالحاجة المُلحة نفسه، تماما مثل الاجتماع الذي كان قد دعا إليه في أعقاب تدريب «المتلقي المؤهل»، وسأل الضباط من حوله السؤال ذاته الذي كان قد طرحه من قبل: «من الذي يتولى زمام الأمور؟»[8].

خفض الجميع نظرهم إلى أحذيتهم أو إلى دفاتر تدوين ملاحظاتهم، لأنه في الواقع، لم يكن شيء قد تغير؛ لم يكن أحد مسؤولا حتى تلك اللحظة. ربما كانت أجهزة أنظمة كشف التسلل قد وُضِعت في أماكنها، لكن لم يكن أحد قد أصدر نُظُما أو أساليب بشأن ما ينبغي فعله إذا انطلقت صافرات الإنذار، أو كيف يُمكن التمييز بين مزحة مزعجة واعتداء جاد خطير.

في النهاية، رفع يده البريجادير جنرال (العميد) جون سوب كامبل، قائد الوحدة السرية جيه - 39، الذي كان في تدريب «المتلقي المؤهل»، وهو رجل هيئة الأركان المشتركة المكلف، وقال: «أنا المسؤول»، على الرغم من أنه لم يكن لديه أي فكرة ما الذي كان ربما يعنيه ذلك.

بحلول الوقت الذي بدأ فيه هجوم «متاهة ضوء القمر» يسبب إثارة الفوضى، كان كامبل يضع خططا لإنشاء مكتب جديد يُدعى «فريق العمل المشترك لحماية شبكات الحاسوب» (جيه تي إف - سي إن دي). كانت أوامر إنشاء فريق العمل قد وُقِّع عليها في 23 يوليو، وكان قد بدأ عملياته في 10 ديسمبر. كان المكتب الجديد مزودا بثلاثة وعشرين ضابطا فقط، يمثلون مزيجا من متخصصي الحاسوب ورجال عمليات الأسلحة التقليدية الذين كان يتحتم عليهم تلقي دورة مكثفة بشأن الموضوع، تكدسوا جميعا داخل عربة مقطورة إيواء، خلف مقر وكالة نظم معلومات الدفاع في ضواحي فيرجينيا Virginia بالقرب من البنتاغون. كان جهدا متواضعا على نحو سخيف من أجل جماعة كانت، وفقا لميثاقها، ستصبح «مسؤولة عن تنسيق[9] وإدارة الدفاع عن أنظمة وشبكات الحاسوب في وزارة الدفاع»، بما في ذلك «تنسيق الإجراءات الدفاعية في وزارة الدفاع» مع «دوائر حكومية أخرى ومع مؤسسات القطاع الخاص ذات العلاقة».

كانت خطوات كامبل الأولى ستبدو لاحقا أنها أولية، لكن لم يكن أحد قط قد اتخذ مثلها على مثل هذا النطاق الواسع، وعدد قليل كان قد فكر فيها هكذا. لقد أنشأ كامبل مركزا للمراقبة يعمل على مدار الساعة وطوال أيام الأسبوع (7/24)، ووضع نظما (بروتوكولات) ينبه من خلالها كبار المسؤولين والقادة الميدانيين إلى وجود تسلل سيبراني، وكانت أولى خطواته هي أنه - على مسؤوليته الخاصة - أرسل بلاغا إلى جميع مسؤولي وزارة الدفاع ينصحهم بتغيير كلمات المرور الخاصة بحواسيبهم.

عند هذه النقطة، كان هجوم «متاهة ضوء القمر» مستمرا طوال أشهر عدة، وكانت نوايا ومنشأ المتسللين لاتزال محيرة. معظم التسللات التي لوحظت كانت تحدث في فترة الساعات التسع نفسها. تماما مثلما كانوا قد فعلوا في أثناء هجوم «الشروق الشمسي»، نظر بعض محللي الاستخبارات بالبنتاغون ومكتب التحقيقات الفدرالي إلى خريطة النطاق الزمني، وأجروا بعض العمليات الحسابية، وخمَّنوا أن المهاجم ينبغي أن يكون في موسكو. ثمة آخرون في وكالة الأمن القومي، لاحظوا أن طهران في منطقة زمنية مجاورة وساقوا حججا تؤيد أن إيران هي موطن مُختَرِق الحاسوب (الهاكر).

في تلك الأثناء، كان مكتب التحقيقات الفدرالي يتقصى جميع الأدلة[10]. كان مُختَرِق الحاسوب (الهاكر) قد قفز وتنقل عبر حواسيب أكثر من اثنتي عشرة جامعة، كان من بينها جامعات سينسيناتي Cincinnati، وهارفارد Harvard، وبرين ماور Bryn Mawr، وديوك Duke، وبيتسبيرغ Pittsburgh، وأوبورن Auburn. أرسل مكتب التحقيقات الفدرالي عملاء إلى كل حرم جامعي لمقابلة الطلاب، والعاملين التقنيين، وأعضاء هيئة التدريس. وجِّهَت أصابع الاتهام إلى بضعة من المشتبه فيهم هنا وهناك، مثل: أحد مساعدي تكنولوجيا المعلومات أجاب عن الأسئلة بعصبية، وطالبة لها صديق أوكراني. لكن لم تؤدِ أي من هذه الخيوط إلى أي نتيجة. لم تكن كليات الجامعات هي مصدر الاختراق، كانت مثل مركز لورانس بيركلي للحاسوب في كتاب «كليف ستول» بيضة طائر الوقواق، لم تكن سوى نقاط عبور ملائمة للقفز من موقع مستهدف إلى موقعٍ آخر.

في نهاية المطاف، كانت هناك ثلاث طفرات باهرة مفاجئة حدثت على نحو مستقل بعضها عن بعض. كانت إحداها مُستوحاة من كتاب ستول. قبل ذلك باثني عشر عاما، كان ستول قد اصطاد مُختَرِق الحاسوب الألماني الشرقي عن طريق تخليق «وعاء عسل»، وهو مجموعة من ملفات زائفة مخادعة، زاخرة بأدلة (فهارس)، ومستندات، وأسماء مستخدمين، وكلمات مرور، جميعها من اختراع ستول، وكانت تبدو ظاهريا أنها ذات علاقة بالبرنامج الأمريكي للصواريخ الدفاعية، وهو موضوع له أهمية خاصة لدى مخترق الحاسوب. حالما كان «وعاء العسل» يستدرج مخترق الحاسوب، فإنه كان يمكُث في مكانه فترة طويلة بما يكفي للسلطات أن تتعقبه وتتتبع تحركاته. قررت مجموعة الاستخبارات المشتركة بين الوكالات المسؤولة عن حل قضية «متاهة ضوء القمر»، وهي في الأساس محللو وكالة الأمن القومي الذين يعملون تحت رعاية وكالة الاستخبارات المركزية، قررت فعل ما كان ستول قد فعله. خلّقوا «وعاء عسل»، كان في هذه الحالة عبارة عن موقع زائف على الإنترنت (موقع ويب) بشأن برنامج طائرات تجسس أمريكية، حسبوا أنه ربما يُغري مخترِق الحاسوب؛ وتماما مثلما حدث في مُخطط ستول، بلع المختَرِق الطعم. كان الجميع في مجال السيبرانية مفتونا بكتاب «بيضة طائر الوقواق». بعد فترة وجيزة من نشر كتابه، كان ستول، وهو هيبي

ذو شعر طويل من بيركلي، قد استُقبل كالأبطال حينما جاء إلى مقر وكالة الأمن القومي لإلقاء كلمة.

لكن محللي وكالة الأمن القومي، وبما كان لديهم من إمكانية استثنائية للحصول على أدوات ومعدات غير مألوفة، أضافوا خطوة أخرى إلى خدعة ستول. حينما غادر مختَرِق الحاسوب موقع الويب، فإنه من دون أن يدرك أخذ معه أداة إرشادية تنبيهية رقمية (بيكون رقمي)، عبارة عن بضعة أسطر من التعليمات البرمجية (الكود)، مرفقة بحزمة البيانات، كانت ترسل إشارة كان المحللون سيمكنهم تتبعها بينما هي تحوم في الفضاء السيبراني. كانت الأداة الإرشادية التنبيهية الرقمية (البيكون الرقمي) نموذجا تجريبيا؛ كانت في بعض الأحيان تعمل، وأحيانا أخرى لا تعمل، لكنها كانت تعمل على نحو جيد بما كان يكفي لأن يتعقب المحللون المخترق إلى عنوان إنترنت IP address يخص «أكاديمية العلوم الروسية» في موسكو.

ظل بعض محللي الاستخبارات، بما في ذلك وكالة الأمن القومي، متشككين، بدعوى أن عنوان موسكو لم يكن إلا نقطة قفز أخرى على طول الطريق إلى الموطن الفعلي للمختَرِق في إيران.

ثم جاءت الطفرة الباهرة الثانية. بينما كان سوب كامبل يعمل على تشكيل «فريق العمل المُشترك لحماية شبكات الحاسوب» (جيه تي إف-سي إن دي)، كان قد عين ضابطا من استخبارات سلاح البحرية يُدعى روبرت غورلي Robert Gourley ليكون رئيسا لاستخبارات فريق العمل. كان غورلي محللا طموحا وقوي الإرادة، ولديه خلفية في علوم الحاسوب. في الأيام الأخيرة للحرب الباردة، كان غورلي قد عمل في إحدى الوحدات التي دمجت الاستخبارات مع العمليات لتعقب الغواصات الروسية ومطاردتها بضراوة. كان غورلي قد تعلم هذا النهج الاندماجي قبل ذلك بخمسة أعوام في دورة تدريبية ميدانية للضباط، اضطلع بتدريسها بيل ستوديمان وريتش هافر، رجلا الاستخبارات القدامى اللذان - قبل ذلك بعقد من الزمان، وتحت إمرة الأدميرال بوبي راي إنمان - دُفعا إلى تبني وسائل الحرب المضادة للقيادة والسيطرة.

قبل وقت قصير من انضمامه إلى فريق العمل مع كامبل، حضر غورلي يوما واحدا مؤتمرا آخر عن عمليات واستخبارات سلاح البحرية. تصادف أن ستوديمان وهافر كانا من بين محاضري ذلك المؤتمر. بعد انتهاء المؤتمر، ذهب غورلي إليهما للتعرف عليهما

شخصيا. بعد بضعة أسابيع، محتجبا داخل غرفة مكتبه بفريق العمل، أجرى غورلي اتصالا هاتفيا مع هافر على خط آمن، وأوضح له مشكلة «متاهة ضوء القمر»، وكذلك الجدال الدائر حول هوية المتسللين، وسأل عما إذا كانت لديه نصيحة بشأن كيفية حل هذه المعضلة.

استحضر هافر فترة الحرب الباردة، وأشار إلى أن وكالة التجسس العسكرية السوفييتية «كيه جي بي KGB» أو «جي آر يو GRU»، كانت عادة ما توفد العلماء إلى المؤتمرات الدولية لجمع أوراق بحثية بشأن ما يهمهم من موضوعات. من ثم، شكَّل غورلي فريقا صغيرا من محللي مختلف دوائر الاستخبارات، ومشطوا السجلات الخاصة بهجوم «متاهة ضوء القمر» لمعرفة الموضوعات التي كان هذا المختَرِق يهتم بها. تبيَّن أن الرقعة كانت تغطي نطاقا واسعا على نحو شديد الغرابة، لم يكن فقط علم الطيران (موضوع بحثه الأول في قاعدة «رايت – باترسون» الجوية)، بل أيضا الهيدروديناميكا (الهيدروديناميات)، وعلم المحيطات، وبيانات مقياس ارتفاع الأقمار الاصطناعية الجيوفيزيقية، والكثير من التكنولوجيا المتعلقة بالتصوير الاستطلاعي. بعد ذلك، فحص فريق غورلي بنوك البيانات الخاصة بالمؤتمرات العلمية التي عُقدت أخيرا. كان التوافق على الأقل مثيرا للفضول، كان علماء روس قد حضروا مؤتمرات عن جميع الموضوعات التي كانت تجذب مختَرِق الحاسوب.

استنتج غورلي من ذلك، بالإضافة إلى برهان وعاء العسل وغياب علامات تشير إلى إيران أو أي مصدر شرق أوسطي آخر، أن الجاني كان روسي الجنسية. إنها كانت تهمة صارخة ومقرِّعة، دولة قومية كانت تخترق الشبكات العسكرية الأمريكية، ولم تكن أي دولة قومية، بل عدو سابق لأمريكا، ومن المفترض أن تكون في الوقت الحالي شريكا بعد انتهاء الحرب الباردة.

أحضر غورلي استنتاجه إلى كامبل، الذي صُدِم، وسأل: «هل تقول إننا نتعرض لاعتداء؟ هل يجب علينا أن نُعلن الحرب؟».

أجاب غورلي، قائلا: «لا، لا». كان هذا تقديرا استخباراتيا، على رغم أنه أضاف أنه كانت لديه «ثقة كبيرة» بدقته.

كانت الطفرة الاستخباراتية الثالثة هي الأقوى والأحدث أيضا، وهي الإنجاز الذي كان يعتمد على أساليب استثنائية ينفرد بها العصر السيبراني، ومن ثم لم يبرع

فيها سوى بضعة مُتخصصين ناشئين. كان كيفن مانديا Kevin Mandia ضمن فريق صغير لمكافحة الجريمة السيبرانية في مكتب التحقيقات الخاصة في سلاح الجو. كان قد زار مِرارا مركز سلاح الجو لوسائل حرب المعلومات في سان أنطونيو، وقد كان مجاريا لنظام رصد أمن الشبكات الذي لدى المركز. حينما بدأ اعتداء «مَتَاهَة ضوء القمر»، تم إيفاد مانديا، وكان حينئذ هو أحد مُقاولي (مُتعهدي) القطاع الخاص، إلى فريق عمل مكتب التحقيقات الفدرالي لفحص ومراجعة سجلات logs مختَرِق الحاسوب الذي كان يستخدم تعليمات برمجية (كود) مبهمة ومُبَالَغا في تشفيرها. كتب مانديا وفريقه برمجية جديدة حديثة لفك تشفير الأوامر، وتبيَّن أن برمجية المختَرِق كتبت باللغة السيريلية (السلافية). استنتج مانديا أن مختَرِق الحاسوب كان روسي الجنسية(*).

طوال الأشهر العديدة الأولى من اعتداء «متاهة ضوء القمر»، عجزت دوائر الاستخبارات الأمريكية عن الإدلاء بأي تصريح بشأن موطن المختَرِق، ولا حتى بصورة غير رسمية. لكن توافق «وعاء العسل» المستوحى من ستول، وتحليل بوب غورلي، وفك الشفرة الذي اضطلع به كيفين مانديا، بدّل المشهد. الحقيقة هي أن هذه الأساليب المتباينة كانت تؤدي إلى النتيجة نفسها. لقد بات جليا أيضا أن قراصنة الحاسوب في عملية «متاهة ضوء القمر»، أيا من كانوا، قد سحبوا غنيمة ثمينة، 5.5 غيغابايت من البيانات[11]، أي ما يعادل ثلاثة ملايين صفحة ورقية تقريبا. لم يكن أي منها مصنفا على أنه سري، لكن كثيرا منها كان حساسا، وربما تُعد إجمالا معلومات سِريَّة إذا ما جمَّعها محلل ماهر وركب بعضها مع بعض.

طوال ما يقرب من العام، فإن فريق العمل بقيادة مكتب التحقيقات الفدرالي - وهو فريق العمل نفسه المشترك بين الوكالات الذي حقق في هجوم «شروق الشمس» – كان قد نسّق التقصي المشترك بين الوكالات، وتشارك كل المعلومات الاستخباراتية، وأحاط البيت الأبيض. في شهر فبراير، أدلى جون هامري بشهادته بشأن هذه المسألة

(*) في العام 2006، كان مانديا سيؤسس شركة تسمى «مانديانت» Mandiant، التي كانت ستبرُز كإحدى الجهات الاستشارية الكبرى المتخصصة في حوادث الأمن السيبراني، وارتقت إلى مكانة بارزة في العام 2011 باعتبارها الشركة التي حددت أن وحدة خاصة في الجيش الصيني هي المُختَرِق (الهاكر) الذي كان وراء مئات الهجمات السيبرانية ضد المؤسسات في الغرب.

في جلسات استماع مغلقة. بعد أيام، تسربت الأخبار إلى الصحافة[12]، بما في ذلك الاستنتاج القائل إن قراصنة الحاسوب (الهاكرز) كانوا من جنسية روسية.

عند هذه النقطة، اقترح بعض أعضاء فريق العمل، لا سيما المنتمون إلى مكتب التحقيقات الفدرالية، إرسال وفد إلى موسكو ومواجهة المسؤولين الروس. ربما يتبيَّن أنه لم تكن لهم صِلة بالاختراق (كان هامري قد شهد بأنه من غير الواضح ما إذا كان قراصنة الحاسوب يعملون لدى الحكومة)، وفي هذه الحالة كان الكرملين ووزارات الأمن سيرغبون في معرفة من هم المارقون في صفوفهم؛ أو ربما كانت الحكومة الروسية ضالعة، وهذه الحالة أيضا كانت تستحق المعرفة.

كان أعضاء فريق العمل المنتمون إلى البنتاغون وإلى وكالة الأمن القومي حذرين بشأن الظهور العلني. ربما لم يكن الروس قد قرأوا التقارير الإخبارية، أو ربما قد قرأوها ولكنهم نبذوها باعتبارها غير صحيحة. بعبارة أخرى، ربما كان الروس لايزالون يجهلون أننا توصلنا إليهم، وأننا كنا نخترق قراصنتهم. وفي أثناء ذلك، كنا نعلم أشياء بشأن اهتماماتهم وأسلوبهم العملياتي. ربما كانت المواجهة الرسمية ستفسد العملية.

في نهاية المطاف، وافق البيت الأبيض على طلب مكتب التحقيقات الفدرالي لإرسال وفد. بعد ذلك، أمضى فريق العمل أسابيع في مناقشة ما هو البرهان الذي سيكون مسموحا للروس بالاطلاع عليه، وما هو البرهان الذي يجب حجبه عنهم. في جميع الأحوال، كان سيُقدَّم إلى الروس بالتعبيرات ذاتها التي استخدمها رسميا مكتب التحقيقات الفدرالي، ليس باعتبارها مسألة تتعلق بالأمن القومي أو الدبلوماسية، بل بوصفه تحقيقا جنائيا، حيث تسعى الولايات المتحدة إلى الحصول على مساعدة من الاتحاد الروسي.

رسميا، أُطلق على الوفد مجموعة تنسيق عملية «متاهة ضوء القمر»، وكان يتألف من أربعة مسؤولين رسميين من مكتب التحقيقات الفدرالي، وهم: عميل ميداني من مكتب «بالتيمور» Baltimore، وخبيران في اللسانيات من سان فرانسيسكو San Francisco، ومشرف من المقر الرئيسي، بالإضافة إلى أحد علماء وكالة الفضاء الأمريكية (ناسا)، وضابطين من مكتب التحقيقات الخاصة في سلاح الجو، كانا قد فحصا مع كيفن مانديا سجلات logs مخترِق الحاسوب. طار الوفد إلى

موسكو في 2 أبريل[13]، حاملا معه الملفات الخاصة بخمس عمليات اختراق سيبراني، وكان من المخطط بقاء الوفد ثمانية أيام.

كان هذا هو عصر العلاقات الودودة بين بيل كلينتون ورئيس روسيا الإصلاحي بوريس يلتسين Boris Yeltsin. لذلك، استُقبلت المجموعة بحفاوة وروح احتفالية، وكان يومهم الأول في موسكو ممتلئا بالأنخاب، والفودكا، والكافيار، والبهجة. أمضى الوفد يومه الثاني في مقر وزارة الدفاع الروسية، في جلسة عمل متصلة. كان الجنرال الروسي، مسؤول الاتصال بالمجموعة، متعاونا جدا، وأخرج السجلات the logs التي تخُص الملفات التي قد أحضرها الأمريكيون معهم. كان هذا إقرارا وتأكيدا بأن الحكومة الروسية كانت هي المختَرِق، وكانت تعمل من خلال مخدمات أكاديمية العلوم. كان الجنرال محرَجًا، وألقى باللوم على «أولاد العاهرة في الاستخبارات».

كاختبار، لربما كان هذا مكيدة، أشار أحد أعضاء الوفد من مُحققي سلاح الجو إلى اقتحام سادس، اقتحام لم تكن المجموعة قد أحضرت ملفاته معها. أخرج الجنرال تلك السجلات أيضا. جأر الجنرال الروسي، وصاح في أصدقائه الأمريكيين الجدد غاضبا، إن هذا عمل إجرامي، ونحن لن نتهاون في هذا.

كان الأمريكيون راضين ومسرورين. كان هذا نجاحا للأمور على نحو استثنائي، ربما كان من الممكن أن يُسوى الأمر كله من خلال الدبلوماسية الهادئة وروح التعاون الجديدة.

في اليوم الثالث، أخذت الأمور منعطفا متقلقلا غير جدير بالثقة. فجأة، أعلن مرافقو المجموعة أن اليوم سيكون لمشاهدة المعالم السياحية، وكذلك كان اليوم الرابع. في اليوم الخامس، لم يكن هناك على الإطلاق توقيتات محددة لأي فعاليات مُجَدوَلة. احتج الأمريكيون برفق بصورة مهذبة، لكن من دون جدوى. لم تطأ أقدامهم ثانية مقر وزارة الدفاع الروسية، ولم يسمعوا ثانية عن الجنرال الذي قدم إليهم العون.

في 10 أبريل، وبينما كان الوفد يستعد للعودة إلى الولايات المتحدة، أكد لهم ضابط روسي أن زملاءه قد شرعوا في إجراء تحقيق دقيق، وكانوا عما قريب سيرسلون خطابا إلى السفارة يوضح ما توصلوا إليه من نتائج.

طوال الأسابيع القليلة اللاحقة، كان المُلحق القانوني في السفارة الأمريكية يتصل بوزارة الدفاع الروسية يوميا تقريبا، مُستفسرا عما إذا كان قد كتب الخطاب، وعلى نحو مهذب طُلب منه أن يكون صبورا. لم يصل أي خطاب البتة. وبدا أن الجنرال الذي قدم لهم العون قد اختفى.

بالعودة إلى واشنطن، حذَّر أحد أعضاء فريق العمل من استنباط استنتاجات فَظَّة، وقال، ربما كان الجنرال مريضا فقط.

بعض من أعضاء البنتاغون ومن دوائر الاستخبارات، الذين كانوا قد حذّروا من الرحلة، قلبوا أعينهم تعبيرا عن الضيق ونفاد الصبر. قال بوب غورلي: «نعم، ربما تكون لديه حالة من التسمم بالرصاص».

كان توافق الآراء الآخذ في الظهور هو أن الجنرال لم يكن على علم بعملية الاختراق، وأنه كان حقا يعتقد أن بعض العناصر المتمردة في الاستخبارات العسكرية هي المتورطة في هذه المكيدة، إلى أن وجّه رؤساؤه الانتقادات إليه، ومن المحتمل أن يكونوا فصلوه من الخدمة، أو أسوأ من ذلك، لإفشائه أسرارا مع الأمريكيين.

ثمة شيء واحد جيد كان ثمرة الرحلة، وهو أن الاختراق بدا كأنه قد توقف.

لكن، بعد مُضي شهرين، اكتشف فريق العمل المشتَرَك لحماية شبكات الحاسوب (جيه تي إف - سي إن دي) في إدارة سوب كامبل جولة أخرى من اختراق مخدمات عسكرية حساسة. كانت لتلك التسللات بصمة مُختلفة بعض الشيء، إذ كانت مصحوبة بتعليمات برمجية (كود) من الصعب كسرها.

عادت لعبة القط والفأر مُجددا. كانت لعبة يضطلع فيها كلا الجانبين، وقريبا دول أخرى، في آن واحد بدور القط ودور الفأر. إلى حدٍ غير معروف إلا لعدد ضئيل من الضباط الأمريكيين، وعدد أقل من كبار المسؤولين السياسيين، ومن دون شك بعض الجواسيس الروس أيضا. كان المحاربون السيبرانيون الأمريكيون يمارسون الهجوم بالإضافة إلى الدفاع، وقد كانوا كذلك فترة طويلة.

6

المُنَسِّق يُقابل «مَادج»

في أكتوبر من العام 1997، قبل بضعة أشهر من اعتداء «الشروق الشمسي»، حينما أصدرت لجنة «مارش» تقريرها بشأن البنى الأساسية الحرجة للبلاد، لم يكن أي شخص مذهولا مما توصلت إليه اللجنة من نتائج أكثر من أحد مُعاوني البيت الأبيض، ويُدعى ريتشارد آلان كلارك Richard Alan Clarke، سوى بضعة مسؤولين.

كان كلارك - بوصفه مستشارا للرئيس كلينتون لمكافحة الإرهاب - قد اشترك في المباحثات رفيعة المستوى التي جرت بعد تفجير مدينة أوكلاهوما سيتي، وما تلاها من إعداد مُسَوَّدة للتوجيه «بي دي دي - 39» (PDD-39) الذي أصدره كلينتون بشأن مكافحة

«كانت «مجموعة بوسطن» فريقا من عباقرة الحاسوب غريبي الأطوار، وكانوا أحيانا يساعدون في تحقيقات إنفاذ القانون»

الإرهاب، ذلك التوجيه الذي أدى في نهاية المطاف إلى تشكيل لجنة «مارش». بعد ذلك، عاد كلارك إلى أعماله الروتينية المعتادة، التي كانت في الأساس تتضمن تَعَقُّب الجهادي السعودي «أسامة بن لادن».

ثم صدر تقرير «مارش»، وكان معظمه يتناول الأمن السيبراني. كان كلارك بالكاد قد سمع عن الأمن السيبراني، إذ لم يكن الموضوع من شأنه. كان راند بيرز Rand Beers - الصديق المقرب إلى كلينتون ومستشاره لشؤون الاستخبارات، هو الرجل المسؤول في اللجنة، وكذلك كان من المفترض أنه سيستعرض التقرير. لكن بُعيد صدور التقرير، أعلن بيرز أنه سينتقل إلى وزارة الخارجية. كان بيرز قد تناقش مع ساندي بيرغر Sandy Berger، مستشار كلينتون للأمن القومي، بشأن من الذي كان ينبغي أن يحل محله في السَبق السيبراني، واستقروا على أنه كلارك.

أبدى كلارك مُمانعة، إذ إنه كان مشغولا بما فيه الكفاية في تَعَقُّب بن لادن. ثم مُجددا، ربما تحول الأمن السيبراني إلى أمر مثير للاهتمام، لقد كان كلارك هو رجل البيت الأبيض المسؤول عن تدريب «المُتَلَقِّي المُؤَهَّل»، وكان كين مينيهان، مدير وكالة الأمن القومي الذي كان قد ابتكر تدريب «المُتَلَقِّي المُؤَهَّل»، قد أطلعه مَلِيًّا على نتائجه وتداعياته. لكن كلارك لم يكن يعرف سوى القليل بشأن الحواسيب أو الإنترنت. لذلك، جمع بضعة موظفين من طاقمه وأخذهم في جولة.

بعد انتهاء العطلات بفترة وجيزة، طاروا إلى الساحل الغربي الأمريكي، حيث زاروا كبار المسؤولين التنفيذيين في كُبرى شركات الحواسيب والبرمجيات. كان أكثر ما أصاب كلارك بالدهشة هو أن مديري شركة مايكروسوفت Microsoft كانوا يعرفون كل شيء بشأن نظم التشغيل، وأولئك في شركة سيسكو Cisco كانوا يعرفون كل شيء بشأن الموجهات routers، وأولئك في شركة إنتل Intel كانوا يعرفون كل شيء بشأن الرقائق، لكن لم يبدُ أن أحدا منهم يعرف الكثير بشأن التجهيزات التي يصنعها الآخرون، أو نقاط الضعف والثغرات الأمنية في التَّماس بينها.

في السابق في واشنطن، طلب كلارك من مينيهان أن يسمح له بجولة في وكالة الأمن القومي. كان كلارك عنصرا فاعلا في سياسة الأمن القومي طوال أكثر من عقد من الزمان منذ إدارة ريغان، لكن في معظم ذلك الوقت، كان قد شارك في المحادثات السوفييتية الأمريكية بشأن الحد من الأسلحة وأزمات الشرق الأوسط، تلك القضايا

البارزة ذات الاهتمام. لم يكن لدى كلارك مُطلقا سبب لزيارة «فورت ميد» أو يلقي بالا بشأنها. أخبر مينيهان مساعديه بأن يُقدموا إلى كلارك عرضا مستفيضا كاملا.

كان جزء من الجولة يعرض مهارة فرق استخبارات الإشارة (سيجينت) في النفاذ بسهولة إلى أي شبكة حواسيب أجنبية تضع أعينها عليها. لم يبعث أي من هذه العروض الطمأنينة في نفس كلارك، لقد بات متقلقلا ومتزعزعا أكثر من قبل، للسبب نفسه الذي عاناه الكثير من المسؤولين الذين كانوا قد شاهدوا عروضا مماثلة عبر السنين. لقد أدرك كلارك أنه إذا كان بإمكاننا فعل ذلك بدول أخرى، فإنهم قريبا سيمكنهم فعل الشيء نفسه بنا. وكان هذا يعني أننا في مأزق وكنا مخدوعين، لأنه لم يكن ممكنا تأمين أي شيء على الإنترنت، وكما أوضح تقرير «مارش» بمزيد من التفصيل، كان كل شيء في أمريكا يحدث على الإنترنت.

كان كلارك يرغب في معرفة مدى ضعف شبكات الحواسيب في أمريكا في الوقت الحالي، وكم هي عُرضة للهجوم، وظن أن أفضل طريقة لاكتشاف ذلك هي التحدث مع بعض قراصنة الحواسب (الهاكرز). على الرغم من ذلك، لم يكن يرغب في التعامل مع مُجرمين، لذا اتصل بصديق له يعمل في مكتب التحقيقات الفدرالي، وسأله إن كان يعرف أيا من قراصنة الحاسوب الأخلاقيين غير الأشرار. عند هذه النقطة، لم يكن كلارك يعرف ما إذا كانت مثل هذه المخلوقات موجودة بالفعل. في البداية كان العميل الفدرالي مُحجِما عن تَشَارُك مصادره، لكن في نهاية المطاف أوصل كلارك بما أسماه «مجموعة بوسطن»، وهو فريق من عباقرة الحاسوب غريبي الأطوار، كانوا أحيانا يساعدون في تحقيقات إنفاذ القانون، وكانوا يُطلقون على أنفسهم اسم «لوفت L0pht»(*).

كان الرجل الممثِّل لمجموعة «لوفت»، الذي كان سيُعرف باسم مادج Mudge، سيقابل كلارك في أحد الأيام في الساعة السابعة مساء، في مصنع جون هارفارد John Harvard لتصنيع الجِعة، بالقرب من ميدان هارفارد في مدينة كامبريدج. في اليوم المحدد، طار كلارك إلى بوسطن، واستقل سيارة أجرة إلى الحانة، ووصل إلى هناك عند تمام الساعة السابعة مساء. مكث كلارك هناك مدة ساعة في انتظار أن يقترب

(*) لوفت L0pht، باللغة العربية تعني الغرفة العلوية (سندرة) أو شرفة في دور علوي. [المُترجم].

منه أحد، لكن أحدا لم يفعل، لذا نهض كلارك وهَمَّ بالرحيل، حينئذ لمس مِرفقه الرجل الذي كان يجلس إلى جواره في هدوء، وقال: «مرحبا، أنا مادج».

تفحصه كلارك. بدا أن الرجل في نحو الثلاثين من عمره، وكان يرتدي سروالا من الجينز، وقميصا قصير الكمَّين (تي شيرت)، وقرطا واحدا، وكان ذا عُثْنُون (لحية صغيرة على الذقن)، وشعر ذهبي طويل («مثل يسوع»، كما كان سيذكره كلارك لاحقا).

سأله كلارك: «منذ متى وأنت تجلس هناك؟».

أجاب مادج: «منذ نحو ساعة». لقد كان هناك طوال الوقت.

تجاذبا أطراف حديث عرضي بشأن «لوفت» مدة نصف ساعة أو نحو ذلك؛ وعند تلك اللحظة، سأل مادج عما إذا كان كلارك يرغب في مُقابلة بقية المجموعة، فأجاب كلارك: بالتأكيد. قال مادج إنهم هناك، مُشِيرا إلى طاولة كبيرة في الزاوية حيث كان يجلس ستة رجال، جميعهم في العشرينيات أو أوائل الثلاثينيات من العمر، بعضهم جامح ومُنفلت تماما مثل مادج، وآخرون مُهَندَمون.

قدمهم مادج بأسمائهم المستعارة: براين أوبليفين Brian Oblivion، وكينغبين Kingpin، وجون تان John Tan، وسبايس روج Space Rogue، وويلد بوند Weld Pond، وستيفان فون نيومانStefan von Neumann.

بعد مزيد من الأحاديث القصيرة، سأل مادج عما إذا كان كلارك يرغب في رؤية «لوفت»، فأجاب كلارك: نعم بالتأكيد. من ثم قطعوا مسافة عشر دقائق بالسيارة إلى مكان بدا كأنه مستودع مهجور في مدينة ووترتاون Watertown بالقرب من نهر تشارلز. دخلوا وصعدوا إلى الطابق الثاني، وفتحوا بابا آخر، وأضاءوا الأنوار التي كشفت عن مُختبر عالي التقانة، مُكتظ بالعشرات من الحواسيب المركزية، وحواسيب سطح المكتب، والحواسيب المحمولة، وأجهزة المودم، وبضعة أجهزة راسم الذبذبات (أوسيلوسكوب)، ومعظمها كان متصلا سلكيا بصفيف من الهوائيات وأطباق الاستقبال الموجودة على سطح البناية، مثلما أشار مادج، عندما عادوا إلى الخارج.

سأل كلارك: كيف كان يمكنهم تَحَمُّل تكلفة كل هذه المعدات. قال مادج إنها لم تتكلف الكثير. كان بعضهم يعمل لدى كُبريات شركات الحاسوب بأسمائهم الحقيقية، لذا كانوا يعرفون حينما كانت تلك الشركات تتخلص من الأجهزة، وكانوا

في ذلك اليوم يذهبون إلى صندوق النفايات، ويسترجعون المعدات، ويرممونها ويجددونها.

علم كلارك أن تجمُعهم قد بدأ[1] في أوائل التسعينيات من القرن العشرين، أساسا على أنه مكان حيث يُمكن لأعضائه تخزين أجهزة الحاسوب الخاصة بهم، ومُمارسة الألعاب عبر الإنترنت. في العام 1994 جعلوا منه عملا تجاريا، حيث كانوا يفحصون البرمجيات الجديدة التي تُنتجها كبريات شركات التكنولوجيا، ويُصدرون نشرة تفصيلية بشأن الثغرات الأمنية. كما أنهم صمموا برمجياتهم الخاصة، وباعوها بسعر مُنخَفِض، بما في ذلك برمجية «لوفت كراك» L0phtCrack، وهو برنامج شائع شهير يُتيح لمُشتريه كسر معظم كلمات المرور المخَزَّنة على نظام التشغيل «مايكروسوفت ويندوز» Microsoft Windows. تذمر بعض المديرين التنفيذيين، لكن آخرين كانوا مُمْتَنّين، إذ إن شخصا ما كان سيكتشف تلك العيوب، وعلى الأقل كانت «لوفت» تفعل ذلك في العلن، ومن ثم كانت الشركات تستطيع إصلاح العيوب. لقد أثارت عملية حرب العصابات هذه استغراب كل من وكالة الأمن القومي، ووكالة الاستخبارات المركزية، ومكتب التحقيقات الفدرالي، ومركز سلاح الجو لوسائل حرب المعلومات. بدأ بعض عملائهم وضباطهم بالتحدث مع مادج، الذي كان قد ظهر بصفته مُتحدثا باسم المجموعة، بل حتى إنهم دعوه إلى التحدث في جلسات أمنية رفيعة المستوى.

لم يكن ذلك يعني أن وكالات الاستخبارات في حاجة إلى مادج لإخبارهم بشأن ثغرات البرمجيات التجارية. كان اختصاصيو التشفير في مديرية ضمان المعلومات بوكالة الأمن القومي، يقضون الكثير من وقتهم بحثا عن تلك الثغرات، وكانوا قد اكتشفوا خمسمائة ثغرة أمنية في أول نظام «ويندوز» من شركة مايكروسوفت. وباتفاق رحبت به صناعة البرمجيات في ذلك الوقت، كانوا على نحو دوري يُخبرونهم بشأن ما يتوصلون إليه من نتائج - معظم النتائج. وهم على أي حال، كانوا دائما يتركون بضع ثغرات لتستغلها فرق استخبارات الإشارة التابعة للوكالة؛ لأن الحكومات الأجنبية التي كانوا يتجسسون عليها، كانت هي أيضا قد اشترت هذه البرمجيات. في الأغلب كانت شركات وادي السيليكون متواطئة في ترك أبواب خلفية مفتوحة. مع ذلك، كانت وكالة الأمن القومي وغيرها من الدوائر تهتم بمعرفة الكيفية التي

يتعامل بها أمثال مادج مع المسألة. كان ذلك يمنحهم نظرة متعمقة في الطرائق التي ربما يعمل بها قراصنة الحاسوب الغرباء الآخرون الأكثر خُبثا، وهي طرائق ربما لم يأخذها بعين الاعتبار اختصاصيو الأمن في الوكالة.

كان مادج من جانبه يسعد دائما بتقديم المشورة إليهم، ولم يطلب قط مقابلا لها. لقد كان يُدرك أنه في أي يوم من الأيام، ربما سيأتي رجال المباحث الفدرالية ويطرقون باب المستودع، إذ إن بعض مشروعات عصبة «لوفت» كانت مريبة ومشكوكا في مشروعيتها، وأنه سيكون من المفيد لهم استدعاء مديري دوائر الاستخبارات وأجهزة إنفاذ القانون في البلاد بصفتهم شهود عيان.

طوال الساعات القليلة اللاحقة، في تلك الليلة الشتوية في مدينة ووترتاون Watertown، استحوذت عصبة «لوفت» على اهتمام كبير من كلارك الذي كان يستمع لهم بإنصات، أخبروه عن كل ما كان يُمكنهم فعله، إذا رغبوا. كان بإمكانهم كسر كلمات المرور المُخَزَّنة على أي نظام تشغيل، وليس «مايكروسوفت ويندوز» فقط. وكان بإمكانهم فك تشفير أي اتصالات تتم عبر الأقمار الاصطناعية. وكانوا قد ابتكروا برمجية (لم تكن للبيع أو التوزيع بعد) يمكنها اختراق أي حاسوب خاص، والتحكم فيه من بُعد، للتجسُس على كل ضغطة زر يفعلها المُستَخدِم، أو لتغيير ملفاته، أو إبعاده عن الإنترنت، أو تحريكه في حركة خاطفة ونقله إلى موقع آخر من اختيارهم. كانت لديهم مُعدات خاصة تُمَكنهم من إجراء هندسة عكسية لأي رقاقة إلكترونية، عن طريق إزالة غطاء الرقاقة واستخراج قوالب السيليكون the silicon dice(*). بنبرة خافتة، أخبروه بشأن ما اكتشفوه أخيرا، بما في ذلك أوجه الضعف والثغرات الأمنية في بروتوكول البوابة الحدودية (بروتوكول التوجيه بين البوابات) Border Gateway Protocol(**)، وهو نوع من المُوجِّهات الفوقية supra-router لكل حركة البيانات على الإنترنت، الذي كان سيتيح لهم - أو لبعض قراصنة الحاسوب المَهَرة المتمرسين الآخرين - إيقاف تشغيل شبكة الإنترنت بأسرها في خلال نصف ساعة.

(*) قوالب السيليكون the silicon dice، هي كتلة صغيرة من مادة شبه موصلة مطبوع عليها تصميم الدائرة المتكاملة التي تؤدي وظيفة معينة. [المترجم].

(**) بروتوكول البوابة الحدودية (بروتوكول التوجيه بين البوابات) Border Gateway Protocol، هو بروتوكول توجيه خارجي، مُصمَّم لتبادل المعلومات المتعلقة بالتوجيه بين الأنظمة المستقلة في شبكات الحاسوب. [المترجم].

لم يكن كلارك يعرف ما إذا كان سيُصَدِّق كل ما قالوه، لكنه كان مصدوما ومُتَهَيِّبا. في أثناء دورته التدريبية المُكثَّفة حول أساليب عمل الإنترنت ومثالبها، كان جميع من أطلَعَه قد أشار ضمنا أو أعلن صراحة أن الدول القومية فقط هي التي تمتلك الموارد اللازمة لتنفيذ نصف الأشياء التي كان مادج ورفاقه يقولون - وفي بعض الحالات، كانوا يقدمون بيانا عمليا - إنهم يمكنهم تنفيذها من تلك الفتحة في الجدار، بقليل من المال، ووفقا لما كان يعتقد، من دون دعم خارجي. باختصار، فإن النموذج الرسمي للتهديد بدا أنه خاطئ تماما.

لقد أدرك كلارك، المستشار الخاص للرئيس لشؤون مكافحة الإرهاب، أن هذا الشيء السيبراني كان أكثر من مُجرد تحول مثير أخَّاذ، إنه ينسجم مع اختصاصه بصورة دقيقة. إذا استخدم مادج وجماعته مواهبهم لزعزعة المجتمع والأمن الأمريكي، مُستغلين أوجه الضعف والثغرات الأمنية الحرجة التي كان تقرير «مارش» قد أوجزها، فإنهم سيوصمون بأنهم إرهابيون، إرهابيون سيبرانيون. إذن، كان هنا يكمُن تهديد آخر يجب على كلارك القلق بشأنه، وأن يُضيفه إلى إضبارة مسؤولياته التي تزداد سُمكا وتعقيدا.

بعد بضع كؤوس شراب أخرى، صارت الساعة الثانية صباحا، حينئذ قرروا إنهاء لقائهم. سألهم كلارك عما إذا كانوا يرغبون في الذهاب إلى واشنطن في جولة خاصة بالبيت الأبيض، وعرض أن يتحمَّل هو التكاليف.

دُهش مادج والآخرون. كان مصطلح «قراصنة الحاسوب» - وهم كانوا كذلك - لايزال بغيضا وعدائيا في معظم الأروقة الرسمية. أن يدعوهم شبح (جاسوس) في وكالة مكونة من ثلاثة أحرف لإحاطة غرفة ممتلئة بأشباح آخرين بصورة سرية جدا، كان أمرا يختلف تماما عن دعوتهم إلى البيت الأبيض من قِبَل مُستشار خاص لرئيس الولايات المتحدة.

بعد مُضي شهر، حضروا، ليس فقط لرؤية الجناح الغربي بعد الدوام، ولكن أيضا للإدلاء بشهادتهم أمام الكونغرس. تصادف أن لجنة الشؤون الحكومية في مجلس الشيوخ كانت تعقد جلسات استماع بشأن الأمن السيبراني؛ وباتصالاته في كابيتول هيل (الكونغرس)، استطاع كلارك أن يضع جميع أعضاء «لوفت» السبعة على قائمة الشهود، مُستخدما أسماءهم المستعارة.

في أثناء تلك الفترة، كان كلارك قد أجرى المزيد من الحوارات مع مادج، وتبيَّن أن اسمه الحقيقي هو بيتر زاتكو Peiter Zatko. كان زاتكو قرصان حاسوب[2] منذ بداية سنوات المراهقة. كان يكره فيلم «ألعاب الحرب (المناورات الحربية)» لأنه شجع الكثير من أُناس آخرين في مثل سنه، لكنهم بعيدون جدا عن مُعدَّل ذكائه، على الانضمام إلى المجال. لم يكن زاتكو مُتخرجا في أحد الأماكن مثل «معهد ماساتشوستس للتكنولوجيا»، مثلما كان كلارك يظن، لكن في كلية بيركلي للموسيقى، تخصص الجيتار، وكان من الأوائل على فصله الدراسي. في أثناء النهار، كان زاتكو يعمل اختصاصيا في أمن الحاسوب في شركة «بي إن إن» BNN، وهي شركة مقرها في مدينة كامبريدج؛ وعلى الرغم من شعبيته الوشيكة، فقد أسرع في خططه للاستقالة وتحويل «لوفت» إلى مؤسسة تجارية تعمل بدوام كامل.

وأول ظهور له وأعضاء «لوفت» الآخرين[3] في «كابيتول هيل» (الكونغرس) كان في 19 مايو من العام 1998. لم يكن يحضر جلسة الاستماع سوى ثلاثة من أعضاء مجلس الشيوخ، هم: فرِد تومبسون Fred Thompson (رئيسا)، وجون غلين John Glenn، وجو ليبرمان Joe Lieberman، لكنهم تعاملوا باحترام مع هؤلاء الشهود غير المألوفين، وأشادوا بهم بوصفهم وطنيين، شبههم ليبرمان بـ «بول ريفير» Paul Revere(*)، لتحذيرهم المواطنين من الخطر في العصر الرقمي.

بعد ثلاثة أيام من إدلاء مادج بشهادته[4]، وقَّع كلينتون على القرار الرئاسي التوجيهي «بي دي دي63-»، بعنوان «حماية البنية الأساسية الحرجة»، مُعيدا صياغة نتائج لجنة «مارش» فيما يخُص تزايد اعتماد البلاد على شبكات الحاسوب، وضعف تلك الشبكات في مواجهة الهجوم، ومُلخصا لسُبُل تخفيف حدة المشكلة.

كانت لجنة خاصة في مجلس الأمن القومي، برئاسة راند بيرز، قد أعدت المُسَوَّدات الأولى للتوجيه. بعد ذلك، في أحد الاجتماعات، أخطر بيرز المجموعة بأنه سينتقل إلى وزارة الخارجية، وأن ديك كلارك - الذي كان، لأول مرة، جالسا إلى جواره - كان سيحل محله في المشروع.

(*) بول ريفير Paul Revere، هو صائغ ونقاش فضة أمريكي، وأحد رواد الصناعة في البلاد، وكان أحد الوطنيين في الثورة الأمريكية. اشتهر ريفير برحلته الليلية في أبريل من العام 1775 لينبه ميليشيا المستوطنين من مجيء القوات البريطانية قبل معارك ليكسينغتون وكونكورد، أولى المواجهات العسكرية في الحرب الثورية الأمريكية. [المترجم].

أثار ذلك دهشة واستهجان العديد من المسؤولين في اللجنة. كان كلارك شخصية مندفعة ومتعجرفا، ويتلاعب بسياسات النظام الإداري، ينال إعجاب البعض باعتباره يُعتمَد عليه وقادرا على التنفيذ، ويحتقره آخرون باعتباره مُناورا وبارعا في الكذب من أجل انتزاع السلطة. كان جون هامري، نائب وزير الدفاع، على وجه الخصوص لا يثق بكلارك. سمع هامري مرارا شكاوى من جنرالات من فئة النجمات الأربع، وقادة مقاتلين في الميدان، أن كلارك كان قد اتصل بهم مباشرة ليأمرهم، بدلا من المرور عبر وزير الدفاع، كما كان من المفترض أنه حتى الرئيس يفعل ذلك. ذات مرة في أثناء إحدى الأزمات، أخبر كلارك أحد الجنرالات بأن الرئيس كان يرغب في نقل سَرِيَّة من الجنود إلى الكونغو، نظر هامري في الأمر، واكتشف أن الرئيس لم يكن قد طلب مثل هذا الشيء. (في نهاية المطاف وقع كلينتون على الأمر، لكن بالنسبة إلى هامري وعدد من الجنرالات، لم يكن هذا مبررا لغطرسة كلارك).

كانت لاستياء هامري جذور أعمق. حينما كان هامري مُراقِبا لحسابات البنتاغون، اكتشف في بضع مرات أن كلارك يستحوذ على موازنة الدفاع من أجل «إجراءات الطوارئ»، زاعما أن ذلك نيابة عن الرئيس. وبهدف المناورة، تذرع كلارك بسند قانوني، بند مُبهم مغمور كان قد اكتشفه في قانون المساعدة الأجنبية، القسم 506، والذي كان يسمح للرئيس بتخصيص مبلغ يصل إلى 200 مليون دولار من خزانة الوزارة لتلبية المُتطلبات العاجلة غير المُمَوَّلة. كان لدى هامري ما يكفي من المشكلات التي تُسبب صداعا في الرأس، مُتَعَامِلا مع خفض الموازنة بعد الحرب الباردة، والضغوط من رؤساء الأركان، بخلاف انقضاض كلارك على البنتاغون ومعاملته مثل حصالته الخنزيرية.

نتيجة لذلك، وعلى الرغم من أنه كانت لهما آراء مُتماثلة بشأن العديد من القضايا وليس فقط الأمن السيبراني، كان هامري قد أخفى عن كلارك بعض الأشياء، وكان في بعض الأحيان يُطلِع نواب الوزارة الآخرين على انفراد في جلسة خاصة، بدلا من أن يكون بمُذكِّرة أو في اجتماع مجلس الأمن القومي، من أجل إبقاء كلارك خارج الأمر.

في وقت قريب من هجمات «الشروق الشمسي» و«مَتَاهَة ضوء القمر» تصادف أن مُدعيا خاصا كان يحقق في الاتهامات التي كانت قد وُجهت إلى الرئيس كلينتون

والسيدة الأولى قبل ذلك بأعوام، بأنهما قد انتفعا على نحو غير مشروع من صفقة أرض في ولاية أركنساس Arkansas. خرجت الأوامر من المستشار القانوني للبيت الأبيض بحظر كل الاتصالات بين البيت الأبيض ووزارة العدل إلا من خلاله. تجاهل كلارك الأمر (ذات مرة أخبر محامي وكالة الأمن القومي بأن «الجهاز الإداري (البيروقراطيين) والمحامين يُعرقلون الأمور فقط»)، واستمر في الاتصال بفريق عمل مكتب التحقيقات الفدرالي من أجل الحصول على معلومات بشأن التحقيقات التي يُجريها بشأن الاختراقات. ولم يكن لويس فريه Louis Freeh، مدير المكتب، أيضا يحب كلارك، وطلب من مرؤوسيه أن يتجاهلوا الاتصالات.

لكن كلارك كان لديه حُماةٌ يُقَدِّرون نُصحه وألمعيته. حينما حث رئيس إحدى الدوائر ساندي بيرغر Sandy Berger، مستشار الأمن القومي، على صرف كلارك من الخدمة، أجاب بيرغر: «إنه وغد سافل، لكنه الوغد الخاص بي». أيضا كان الرئيس مستحسنا اضطلاع كلارك بالمراقبة لمصلحته.

كان موظفو المستوى الأوسط متعجبين حقا من الشبكة التي كان كلارك قد نسجها في كل جنبات الجهاز الإداري، ومن إصراره وقدرته على إدارتها. ذات مرة، بعد فترة وجيزة من مجيئه من وكالة الأمن القومي ليكون مستشارا لنائب الرئيس غور لشؤون الاستخبارات، جلس ريتش ويلهلم في اجتماع للمجموعة الفرعية لمكافحة الإرهاب التابعة لمجلس الأمن القومي، وكان كلارك يترأس الاجتماع. كانت طاولة الاجتماع تضم ضباطا ومسؤولين رفيعي المستوى، من جميع الدوائر والوزارات المعنية، وكان هناك كلارك، هذا المدني غير المنتخب وغير المؤكد، يصيح آمرا جنرالا في سلاح الجو للحصول على طائرة غير موسومة بأي علامات، ويملي على وكالة الاستخبارات المركزية عدد العملاء الذين يتعين أن يكونوا على متنها، كل ذلك بسلطة لا نقاش فيها.

أحد معاوني كلارك يدعى جون مكارثي John McCarthy، وهو قائد في خفر السواحل لديه خلفية في إدارة الطوارئ، كان في بدايات توليه القيادة قد حضر اجتماعا بشأن الموازنة عقد في أحد أيام السبت، حيث قام كلارك، فور سماعه أن أحد البرامج المهمة ينقصه 3 ملايين دولار لتلبية احتياجاته، وأمر مكارثي بأن يحصل على المال من شخص بعينه في إدارة الخدمات العامة، مضيفا: «افعل ذلك

يوم الاثنين لأنني في حاجة إليها يوم الثلاثاء». أخبر مسؤول إدارة الخدمات العامة مكارثي بأنه كان سيمنحه 800 ألف دولار، عند هذه النقطة بدأت المساومة. انتهى الأمر بأن حصل كلارك على ما يقرب من المبلغ كاملا.

عندما حل كلارك محل راند بيرز كان نواب الوزراء في مجلس الأمن القومي بصدد إعداد مسودة التوجيه الرئاسي بشأن حماية البنية الأساسية الحرجة، ويتأرجحون جيئة وذهابا متنازعين بشأن عدم الاتفاق والعبارات التوافقية. أخذ كلارك ما نفذوه من عمل، وعاد إلى مكتبه، وكتب المسودة بنفسه. كانت وثيقة تفصيلية، تنشئ محافل عديدة يتعاون فيها القطاع العام مع القطاع الخاص بشأن الأمن السيبراني، كان أبرزها مراكز تشارك وتحليل المعلومات، حيث كانت الحكومة ستدعم الشركات في مختلف قطاعات البنية الأساسية الحرجة (الخدمات المصرفية، والنقل، والطاقة، وما إلى ذلك)، عن طريق تقديم ما لديها من خبرات؛ بما في ذلك، في بعض الحالات، المعارف المصنفة على أنها سرية. بذلك سيمكنهم إصلاح ومعالجة ما لديهم من نقاط ضعف وثغرات أمنية.

وفقا للتوجيه، كما كتبه كلارك، فإن هذا الجهد برمته كان سيترأسه مسؤول جديد هو «المنسق القومي للأمن وحماية البنية الأساسية ومكافحة الإرهاب»، ويُعيَّن من قبل الرئيس. حرص كلارك مسبقا على أنه هو ذاته الذي سيكون هذا المنسق القومي.

كان المنتقصون من قدر كلارك، وبعض من المعجبين به، يرون هذا اختطافا سافرا للسلطة. كان كلارك لديه بالفعل ملف مكافحة الإرهاب، الآن هو سيصبح مسؤولا عن البنية الأساسية الحرجة أيضا. رأى بعض منتقديه، لا سيما في مكتب التحقيقات الفدرالي، أن الفكرة خاطئة من الناحية الموضوعية. تمهيدا، كانت التهديدات السيبرانية تأتي أساسا من الدول القومية ومن المجرمين، وربط القضية بمكافحة الإرهاب كان من شأنه أن يسيء فهم وتفسير المسألة، ويصرف الانتباه عن الحلول الجادة. (كما أن الفكرة كانت تهدد بتهميش مكتب التحقيقات الفدرالي، الذي كان قد اتخذ دورا رئيسيا ومركزيا في «الشروق الشمسي» و«متاهة ضوء القمر»).

أنكر كلارك الاتهامات. أولا، ومثلما كان هو الحال عادة، كان كلارك يعتبر نفسه الأفضل لهذا المنصب، إذ كان يعرف بشأن القضايا أكثر من أي شخص آخر في البيت

الأبيض، كان هو وبيرز الوحيدين اللذين أوليا المشكلة اهتماما كبيرا منذ أن نشأت. ثانيا، أقنعته لقاءاته مع مادج بأن نوعا معينا من الإرهابيين كان يستطيع أن ينجح في هجوم إلكتروني فتاك، ولم يكن كلارك قد أخذ هذه الفكرة بعين الاعتبار من قبل. كان كلارك يوضح ببرود وعقلانية لكل من كان يسأل أنه من المنطقي أن يمدد ملف مسؤولياته في هذا الاتجاه.

كما جرت العادة، حصل كلارك على ما يريده.

لكن التوجيه الذي صاغه كلارك اصطدم بعقبة مع القطاع الخاص. في القسم الرقم 5 من الوثيقة «بي دي دي - 63»، كتب كلارك مُرسيا «المبادئ الإرشادية»: «ستكون الحكومة الفدرالية بمنزلة نموذج للقطاع الخاص بشأن كيفية تحقيق أفضل ضمان للبنية الأساسية، وبقدر المستطاع ستوزع نتائج مساعيها».

كان هذا هو أشد ما يخشاه المديرون التنفيذيون في الشركات، أن تدير الحكومة الأمور. بدقة أكثر، سيكونون مكبلين بأشد الكلمات بغضا في قاموسهم، ألا وهي اللوائح. كانوا قد استشعروا مثل هذا التهديد حينما تقابلوا مع لجنة «مارش»، كان هناك جنرال في سلاح الجو. وعلى الرغم من أنه كان متقاعدا، كان يشير إلى نفسه على أنه الجنرال «مارش»، مرسيا القواعد لما يجب عليهم أداؤه، كأنهم من رجال الجيش المجندين. والآن كان هنا دِك كلارك، يكتب تحت توقيع الرئيس، محاولا إرساء القانون.

لقد كانت تلك الشركات نفسها تعمل مع واشنطن طوال عدة أشهر في تناغم واتساق، وفي إطار مبادئها التوجيهية، من أجل حل أزمة «العام 2000». بزغت هذه الأزمة - المعروفة أيضا باسم «خلل الألفية» - حينما أدرك أحد الأشخاص أنه في بعض برامج الحاسوب الأكثر أهمية في الحكومة كانت السنوات (تواريخ الميلاد، تواريخ التقاعد، فترات الرواتب، وما إلى ذلك) قد رُمِّزت باستخدام الرقمين الأخيرين منها، مثلا: 1995 على أنها 95، و1996 على أنها 96... وما إلى ذلك. حينما كان التقويم سينقلب إلى العام 2000، كانت الحواسيب ستقرأه على أنه 00. وكان الخوف من أن الحواسيب ربما كانت ستفهمه على أنه العام 1900. عندئذ، فإن برامج مثل الضمان الاجتماعي والرعاية الصحية ستتوقف على نحو مفاجئ، فالأشخاص الذين كانوا سيتسلمون الشيكات كان الحاسوب سيعتبرهم غير مؤهلين، لأنهم - بقدر ما

كانت الحواسيب تفهم - لم يكونوا قد ولدوا بعد. ربما تتوقف فجأة دفعات رواتب موظفي الحكومة، بما في ذلك القوات المسلحة. كما أن بعض البنى الأساسية الحرجة، التي لديها برامج رُمِّز فيها الوقت، ربما تتعطل أيضا.

للتعامل مع المشكلة أنشأ البيت الأبيض مركزا قوميا لتنسيق المعلومات لاستحداث إرشادات جديدة للبرمجيات والتأكد من اتساق الجميع. استُدعيَت كبريات الشركات، مثل «إيه تي آند تي» AT&T و«مايكروسوفت» Microsoft، في غرفة واحدة مع مكتب التحقيقات الفدرالي، ووزارة الدفاع، وإدارة الخدمات العامة، ووكالة الأمن القومي، وكل الدوائر ذات العلاقة. لكن المسؤولين التنفيذيين في الشركات أوضحوا أن هذا اتفاق لمرة واحدة، وحالما تُحَلُّ مشكلة العام 2000، سيُفكَك المركز.

كان كلارك يرغب في استدامة هذا النسق وتحويل مركز العام 2000 إلى دائرة تتعامل مع التهديدات السيبرانية. في وقت سابق لم يكن كلارك قد أخفى رغبته في فرض متطلبات إلزامية على الأمن السيبراني للبنية الأساسية الحرجة، وهو كان يعلم أن الشركات الخاصة لم تكن لتنفق الأموال طواعية لاتخاذ الإجراءات اللازمة. لكن مستشاري كلينتون للشؤون الاقتصادية عارضوا الفكرة بشدة، بدعوى أن اللوائح كانت ستُخل بالسوق الحرة وتعيق الابتكار. وافق كلينتون، وتراجع كلارك. كان كلارك حينها ينحت بابا خلفيا، ساعيا إلى تأسيس سيطرة حكومية من خلال نسخة منقحة من مركز العام 2000. كان هذا هو هدفه الخفي من توليه صياغة مسودة التوجيه الرئاسي، ولم تكن الشركات لتقتنع بذلك.

وضعت ممانعة الشركات كلارك في مأزق. كان عاجزا عن فرض اشتراطات صارمة كان الرئيس بالفعل قد ألغاها. وكان في حاجة إلى انضمام القطاع الخاص من أجل إنجاح تفعيل أي سياسة أمنية سيبرانية، إذ إن معظم بيانات الحكومة، بما في ذلك الكثير من البيانات المصنفة على أنها سرية، كانت تتدفق عبر شبكات خاضعة لسيطرة القطاع الخاص. وكما كان تقرير مارش قد أوضح فإن ضعف الكيانات الخاصة - البنى الأساسية الحرجة - كانت له تبعات خطيرة على الأمن القومي.

كان كلارك يدرك أيضا أنه حتى إذا تولت الحكومة الرقابة على حركة البيانات على الإنترنت فإن القليل من الدوائر هي التي تمتلك الموارد أو النبوغ التقني

للاضطلاع بكثير من تلك المهام؛ باستثناء وزارة الدفاع، التي كانت تمتلك السلطة للدفاع عن شبكاتها الخاصة فقط؛ ووكالة الأمن القومي، التي قد استُبعدت مرتين من الاضطلاع بأي دور في رصد الحواسيب أو الاتصالات المدنية؛ أولا، في العام 1984، في أعقاب التوجيه الرئاسي السري المتعلق بالأمن القومي «إن إس دي دي145-» الذي أصدره رونالد ريغان؛ ومجددا، في أوائل فترة رئاسة كلينتون، في أثناء الجدال بشأن «رقاقة كليبر».

قضى كلارك معظم فترة العام ونصف العام اللاحقة بين الأزمات المختلفة المتعلقة بالإرهاب، حيث كتب وثيقة تتكون من 159 صفحة سميت بـ «الخطة القومية لحماية نظم المعلومات: الدفاع عن الفضاء السيبراني لأميركا» (the National Plan for Information Systems Protection: Defending America's Cyberspace)، التي وقَّع عليها الرئيس كلينتون في 7 يناير 2000.

في مسودة أولية كان كلارك قد اقترح تجميع وربط كل الدوائر الحكومية المدنية (غير العسكرية) - ومن المحتمل في نهاية المطاف شركات البنية الأساسية الحرجة - إلى شبكة فدرالية لكشف التسلل أطلق عليها اسم «فيدنت» (FIDNET)[5]. كانت شبكة «فيدنت» ستصير إنترنت موازية، مع مستشعرات (أجهزة الاستشعار) متصلة سلكيا بمرصد إحدى الدوائر الحكومية (لم يوضح أي دائرة). إذا اكتشفت المستشعرات (أجهزة الاستشعار) عملية تسلل، كان سيُنبَّه الراصد بصورة تلقائية مؤللة. كان من الحتمي أن شبكة «فيدنت» ستكون لها بضع نقاط للولوج إلى الإنترنت النظامية، لكن المستشعرات (أجهزة الاستشعار) كانت ستعتلي تلك النقاط، وتنبه المسؤولين للاقتحامات هناك أيضا. أعد كلارك نموذجا للفكرة مستخدما أنظمة كشف التسلل التي رُكِّبت على حواسيب وزارة الدفاع في أعقاب هجوم «الشروق الشمسي». وفي تلك الحالة كانت القوات المسلحة تراقب نفسها، لكن أن ترصد الحكومة المسؤولين المدنيين، فضلا عن القطاع الخاص - وفي ضوء ماهية الدوائر التي كانت تضطلع بهذا النوع من الأمور، التي ربما ستكون هي القوات المسلحة - كان الأمر يُنظَر إليه على نطاق واسع على أنه شيء مختلف ومقيت.

في يوليو من العام 1999 سرَّب أحدهم مسودة كلارك إلى صحيفة «نيويورك تايمز»، وحينئذ امتلأت الأجواء بصيحات الاحتجاج. استنكر الخطة أعضاء بارزون

في الكونغرس وجماعات الحريات المدنية، باعتبارها «أورويلية» (Orwellian)(*) وهدّامة للسلم الأهلي[6]. حاول كلارك إزالة هذه المخاوف، أخبر مراسلي الصحف أن شبكة «فيدنت» لن تنتهك الشبكات الشخصية الخاصة، أو تتعدى على حقوق الخصوصية بأي شكل من الأشكال. كذلك أتت اعتراضات شرسة من المديرين التنفيذيين وأعضاء مجالس الإدارة في شركات البنية الأساسية الذين انتقدوا الخطة بعنف باعتبارها تجسيدا لأسوأ كوابيسهم بشأن لوائح الحكومة.

وُئدت الفكرة؛ وأعيدت كتابة الخطة القومية.

بعد مضي ستة أشهر، حينما انتُهي من مراجعة الخطة القومية وإقرارها، نقش الرئيس كلينتون توقيعه تحت مذكرة إحالة مثيرة، وكان هذا عرفا متواترا معتادا لمثل هذه الوثائق. لكن، وفي خروج عن المألوف، سطر كلارك - باسمه شخصيا - مقدمة منفصلة بعنوان «رسالة من المنسق القومي». حاول فيها أن يمحو صورته المتغطرسة. كتب كلارك: «بينما يستطيع الرئيس والكونغرس إصدار أمر[7] بأن تكون الشبكات الفدرالية آمنة، فإنهم لا يستطيعون ولم يكن ينبغي لهم فرض حلول لأنظمة القطاع الخاص»، كما أنهم «لن ينتهكوا الحريات المدنية، أو حقوق الخصوصية، أو المعلومات المشمولة بحق الملكية». وأضاف: ليس إلا لجعل الأمور أكثر وضوحا، فإن الحكومة «ستتحاشى اللوائح».

ختاما، في مبادرة تصالحية استرضائية جدا، حتى إنها أذهلت الأصدقاء والأعداء على حد سواء، كتب كلارك: «هذا هو الإصدار 1.0 من الخطة. نحن نسعى جادين، ونلتمس وجهات النظر بشأن تحسينها. ونظرا إلى أن كيانات القطاع الخاص تتخذ المزيد من القرارات والخطط للحد مما لديها من أوجه الضعف الأمني وتحسين إجراءات حمايتها، فإن الإصدارات المستقبلية للخطة ستعكس ما يُحرَز من نجاح وتقدم».

بعد مضي شهر واحد حدث أن كبريات الشركات العاملة على الإنترنت في البلاد، بما في ذلك «إيباي» eBay و«ياهوو» Yahoo و«أمازون» Amazon، تعرضت لـ «هجوم حجب الخدمة» (denial-of-service attack). اخترق شخصٌ الآلاف من

(*) أورويلية Orwellian: هي صفة لوصف موقف، أو فكرة، أو حالة اجتماعية وفقا لما حدده الروائي الإنجليزي جورج أورويل George Orwell على أنه أداة لتدمير رفاهة العيش في المجتمعات الحرة والمفتوحة. [المترجم].

حواسيبهم، التي كان عدد منها محميا بشكل أو بآخر، وأغرقها بطلبات لانهائية للحصول على بيانات، مما أدى إلى زيادة تحميل المخدمات إلى النقطة التي تعطلت عندها عدة ساعات، وفي بعض الحالات عدة أيام.

هنا كانت فرصة كلارك لإعطاء دفعة للسياسة القومية، إن لم يكن لإعادة إحياء شبكة «فيدنت» (التي بدت خارج النقاش وأمرا مستبعدا في ذاك الوقت)، فعلى الأقل لفرض بعض القواعد على الجهاز الإداري العنيد وعلى الشركات الضخمة. توجه كلارك مسرعا إلى المكتب البيضاوي، حيث كان كلينتون قد سمع الخبر بالفعل، وقال: «سيدي الرئيس، إن هذا هو مستقبل التجارة الإلكترونية».

أجاب كلينتون، مشتتا بعض الشيء: «نعم، لطالما تحدث غور بشأن التجارة الإلكترونية».

مع ذلك أقنع كلارك الرئيس بعقد قمة[8] في قاعة مجلس الوزراء بالبيت الأبيض، داعيا واحدا وعشرين شخصا من كبار المسؤولين التنفيذيين في كبريات شركات الحواسيب والاتصالات، مثل: «إيه تي آند تي»، و«مايكروسوفت»، و«صن مايكروسيستمز» **Sun Microsystems**، و«هيوليت-باكارد» **Hewlett-Packard**، و«إنتل» **Intel**، و«سيسكو» **Cisco**، إلى جانب حفنة من أبرز رواد البرمجيات اللامعين من شركات الخدمات الاستشارية ومن الأوساط الأكاديمية. كان بيتر زاتكو - الذي أصبح شهيرا الآن - من بين هذه المجموعة، وعرف نفسه في القائمة الرسمية للمدعوين على أنه مادج.

دخل زاتكو إلى اجتماع بانبهار شديد بالمشاهير، من أمثال فينت سيرف **Vint Cerf**، أحد مخترعي الإنترنت، تقريبا بقدر انبهاره برئيس الولايات المتحدة. لكن في أثناء المناقشات، وبعد بضع دقائق من جلوسه، نفد صبره. كان كلينتون مثيرا للإعجاب، يسأل أسئلة ثاقبة تتسم بنفاذ البصيرة، ويستنبط مماثلات صائبة وثيقة الصلة بالموضوع، مستوعبا جوهر المشكلة. لكن مسؤولي الشركات التنفيذيين كانوا يزيفون الأمر، واصفين الهجوم بأنه كان «متطورا جدا»، من دون الاعتراف بأن سلبيتهم هي التي كانت قد سمحت بحدوثه.

قبل ذلك ببضعة أسابيع كان مادج قد أصبح قانونيا[9]. إحدى شركات الإنترنت تسمى «آت ستاك» **@stake**، كانت قد اشترت «لوفت» وحوّلت مستودع مدينة

«واترتاون» Watertown إلى مختبر أبحاث للبرمجيات التجارية للحماية من الفيروسات والمتسللين. مع ذلك لم يكن لدى مادج أي مطامع شخصية في المسرحية التي كانت تتكشف أمام ناظريه، لذلك هو تحدث.

قال: «السيد الرئيس، لم يكن هذا الهجوم متطورا. إنه كان بسيطا بديهيا. كان ينبغي على كل الشركات أن تعرف أن هذا كان سيحدث، لكنها لم تكن قد استثمرت في اتخاذ التدابير الوقائية - التي كانت متاحة في المتناول - لأنهم لم يكن لديهم حافز لتنفيذ ذلك». لم يستفض مادج في توضيح النقطة، لكن الجميع كانوا يعرفون ما الذي كان يقصده بكلمة «حوافز». إذا حدث هجوم فلم يكن أحد سيُعاقب ولم تكن أسعار الأسهم ستنهار، وإصلاح الضرر لم يكن سيتكلف أكثر من تكلفة عرقلة الهجوم ابتداء.

ساد الصمت الغرفة؛ وعلى نحو حاسم، قال فينت سيرف، رائد الإنترنت، «مادج على حق». شعر زاتكو بالزهو، وفي ظل تلك الظروف، شعر بالارتياح.

بينما كان الاجتماع ينفض، والجميع يدردش ويتبادل بطاقات التعريف الشخصية، أشار كلارك إلى زاتكو ليبقى في الجوار. وبعد بضع دقائق ذهب الاثنان إلى المكتب البيضاوي للمزيد من التحدث مع الرئيس. أبدى كلينتون إعجابه بحذاء رعاة البقر الذي ينتعله زاتكو، ورفع حذاءه المصنوع من جلد الثعبان على مكتبه، وكشف عن أنه يمتلك أحذية مصنوعة من كل حيوان ثديي على هذا الكوكب. (قال هامسا: «لا تخبر الليبراليين»). تابع زاتكو مُبادأة الرئيس، الذي انخرط في مزيد من الأحاديث الجانبية. بعد بضع دقائق، وبعد مصافحة وصورة تذكارية، ودع زاتكو الرئيس وخرج من المكتب بصحبة كلارك.

أدرك زاتكو أن الرئيس كان في ذهنه ما يكفي، ما يتعلق بالتداعيات المتواصلة لفضيحة مونيكا لوينسكي Monica Lewinsky (التي كادت تؤدي إلى الإطاحة به)، وتسريع مباحثات السلام في الشرق الأوسط (التي لم تكن ستحرز أي تقدم)، والانتخابات المقبلة (التي كان نائب الرئيس غور ، حامل إرث كلينتون، سيخسرها أمام جورج دبليو بوش الابن).

ما لم يكن زاتكو يعرفه أنه بينما كان كلينتون يستطيع استجماع اهتمام صادق حقيقي بالموضوع - أو بأي موضوع آخر - في اجتماع يضم المديرين

التنفيذيين ذوي النفوذ، فإنه لم يكن يهتم كثيرا بالسيبرانية، والواقع أنه لم يكن قط مهتما بها. كان كلارك هو المرجعية، وغالبا لم يكن للبيت الأبيض مرجع سواه، لأي محرك لهذه القضية.

كان كلارك يعرف أن حديث زاتكو اللاذع في غرفة مجلس الوزراء كان صحيحا ودقيقا. لم يكن المديرون التنفيذيون بالصناعة سيعملون على إصلاح الأمور طواعية. وبهذا المفهوم كان الاجتماع شبه هزلي، مع مناشدة العديد منهم الرئيس أن يتخذ إجراء، ثم في اللحظة التالية، يؤكدون له أنه كان باستطاعتهم التعامل مع المشكلة من دون أمر من الحكومة.

كان كلارك قد أعد إصدارا جديدا من «الخطة القومية لحماية نظم المعلومات» ألطف أسلوبا وأخف حدة، وكان يدعو إلى تنفيذ عدة مشروعات متنوعة لتعاون الحكومة مع قطاع الصناعة الخاص لتنطلق بحلول نهاية العام 2000، وأن تصير جاهزة بالكامل بحلول شهر مايو من العام 2003. لكن الجدول الزمني بدا مستبعدا وغير مقنع. كانت البنوك مقدامة، لقد وافق عدد منها فورا بسهولة على تشكيل مركز على مستوى الصناعة لتشارك المعلومات وتحليلها (آي إس إيه سي) an Information Sharing and Analysis Center (ISAC) للتعامل مع هذا التحدي. لم يكن هذا مستغربا، فقد كانت البنوك هدفا لعشرات من عمليات الاختراق التي كلفتها ملايين الدولارات، وربما كلفتها تزعزُع ثقة كبار العملاء. كان بعض المؤسسات المالية الكبيرة بالفعل قد وظف خبراء اختصاصيين في الحاسوب. لكن معظم البنى الأساسية الحرجة الأخرى، مثل: النقل، والطاقة، والإمداد بالمياه، وخدمات الطوارئ، لم تُخترق بعد، ورأى مسؤولوها التنفيذيون أن هذا التهديد افتراضي ظني. ومثلما كان زاتكو قد لاحظ، فإنهم لم يروا أي حافز يدفعهم إلى إنفاق المال على الأمن.

حتى صناعة البرمجيات تضمنت بضعة راغبين جادين هم الذين عرفوا أن الأمن كان هو المشكلة، لكنهم كانوا يعرفون أيضا أن تنصيب أنظمة آمنة حقا سيؤدي إلى بطء عمليات الخادم، في الوقت الذي يدفع فيه العملاء أموالا كثيرة مقابل المزيد من السرعة. طلب بعض المديرين التنفيذيين من مؤيدي الأمن إجراء تحليل للتكلفة والعائد لمعرفة ما هي أرجحية وقوع حدث كارثي حقيقي، وكم سيكلفهم

مثل هذا الحدث؛ وكم سيتكلف نظام أمني، وما فرص أن يحول النظام حقا دون التسللات؟ لم يكن بإمكان أحد الإجابة عن تلك الأسئلة، لم تكن هناك بيانات لدعم إجابة موثوق بها.

كان فريق عمل شبكة الحاسوب في البنتاغون يواجه عقبات مماثلة. ذات مرة، حينما كان آرت موني Art Money، مساعد وزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات، يجاهد من أجل رفع موازنة أمن الشبكات بنسبة 10 في المائة، سأله أحد الجنرالات عما إذا كان البرنامج سيحقق زيادة في الأمن بنسبة 10 في المائة. جال موني على أصدقائه من التقنيين، في وكالة الأمن القومي وأماكن أخرى، طارحا السؤال. لم يكن أحد يستطيع تقديم أي ضمان من هذا القبيل. كانت الحقيقة هي أن معظم الجنرالات والأدميرالات كانوا يرغبون في مزيد من الدبابات، والطائرات، والسفن؛ مليار دولار إضافي لدرء هجمات الحاسوب - تلك التهديدات التي يعتبرها الكثيرون مستبعدة، حتى بعد تدريب «المتلقي المؤهل»، وتحقيقات «الشروق الشمسي»، وعملية «متاهة ضوء القمر» (لأنها، في نهاية المطاف، لم تكن قد أحدثت أي ضرر ملموس على الأمن القومي) – كانت تعني مليار دولار أقل من أجل الأسلحة.

لكن الأمور كانت تتغير على الجانب العسكري، يرجع ذلك جزئيا إلى أن المزيد والمزيد من الكولونيلات (العقداء)، وحتى بضعة جنرالات، كانوا يشرعون في أخذ المسألة على محمل الجد؛ وجزئيا لأن الوجه الآخر من الأمن السيبراني - الحرب السيبرانية - كان ينطلق بدرجة قصوى.

7

احجب، استغل، أتلف، دمر

«المهاجمون اخترقوا كلمات المرور، واستكشفوا الشبكة، وعثروا على ثغرات نفذوا من خلالها، وحالما صاروا في الداخل استولوا على الشبكة»

عودة إلى صيف العام 1994، بينما كان كين مينيهان ومن لديه في قاعدة «كيلي» الجوية من محترفي استخدام برمجية «عفريت الاتصال الهاتفي» يخططون لإيقاف تشغيل شبكة الهاتف في هايتي توطئة للغزو المرتقب الذي أمر به الرئيس كلينتون، كان ضابط برتبة ليوتينانت كولونيل (مقدم) يدعى والتر داستي رودز Walter Dusty Rhoads يجلس في أحد مراكز القيادة في مدينة نورفولك Norfolk بولاية فيرجينيا Virginia، منتظرا بدء الهجوم.

كان رودز منخرطا في البرامج السوداء (العمليات السرية) لسلاح الجو، بدأ طيارا، أولا على المقاتلة الشبح طراز إف - 117، ثم على طائرات تجريبية مختلفة عدة في مواقع غير معلنة. بحلول موعد حملة هايتي، كان رودز رئيسا لفرع وسائل حرب المعلومات

بقيادة القتال الجوي في قاعدة «لانغلي» الجوية بولاية فرجينيا، وفي هذا الدور، كان قد حول فكرة «مينيهان» للتشويش على الهاتف إلى خطة تفصيلية، ونسّقها مع العمليات الجوية الأخرى.

على مدى أيام عدة، لم يبارح رودز وطاقمه ذلك المكتب في نورفولك، بدأوا يفقدون صوابهم، ويلتهمون بنهم الوجبات السريعة غير المفيدة، وهم يبتدعون كلمات رمزية مشفرة من أجل إعداد خطط احتياطية، في حالة ما إذا سار شيء أو آخر على نحو خاطئ. كانت صناديق الكعكات (بسكويت) من نوع موون باي MoonPie الفارغة، وعلب مشروب فرسكا Fresca الفارغة متناثرة في أرجاء الغرفة، لذلك صاغ رودز منها كلمات رمزية (كودية)، مثل: «فرسكا» Fresca تعني تنفيذ خطة الحرب، «موون باي» MoonPie تعني التراجع.

بعد أن فر الانقلابيون مثيرو الاضطراب في هايتي وأُلغي الغزو، أدرك رودز أن الترتيب كان ملتويا ومعقدا بعض الشيء. كان رودز يعمل من خلال مركز «مينيهان» لوسائل حرب المعلومات التابع لسلاح الجو، الذي كان عبارة عن ورشة استخبارات، وليس قيادة عمليات؛ وبعبارة أدق، كانت الاستخبارات والعمليات القتالية مجالين منفصلين، إذ إن الباب الرقم 10 في مجموعة قوانين الولايات المتحدة يخص القتال، والباب الرقم 50 يخص الاستخبارات. فكر رودز أنه سيكون من الجيد تشكيل وحدة عمليات تابعة لسلاح الجو مُخصَّصة لوسائل حرب المعلومات.

دفع مينيهان بالفكرة في ذلك الخريف، حينما أُعيد انتدابه إلى البنتاغون باعتباره مساعد رئيس الأركان للاستخبارات. كان مينيهان يسوّق الفكرة جيدا. في 15 أغسطس من العام 1995، أصدر كبار المسؤولين أمرا بإنشاء السرب الجوي الرقم 609 لوسائل حرب المعلومات، على أن يكون مقره في قاعدة «شاو» الجوية بولاية كارولينا الجنوبية South Carolina.

جاء في البيان الرسمي أن السرب سيكون «الأول من نوعه[1] الذي يهدف إلى مواجهة التهديد المتزايد لنظم معلومات سلاح الجو». لكن في ذلك الوقت، قليلون هم من كانوا يأخذون أي تهديد من هذا القبيل على محمل الجد. إن تقرير «مارش»، وتدريب «المتلقي المؤهل»، وتحقيقات «الشروق الشمسي»، وعملية «متاهة ضوء القمر» لن يُلطخ أي منها المشهد العام على مدار عامين آخرين. كانت

المهمة الرئيسية الأخرى للسرب، على الرغم من عدم ذكرها في تصريحات علنية، هي استحداث أساليب لتهديد نظم المعلومات لدى خصوم أمريكا.

كان رودز هو الذي سيتولى قيادة السرب، في حين أن ضابط عمليات السرب سيكون ميجور (رائد) يُدعى أندرو ويفر Andrew Weaver. في الربيع السابق، كان ويفر قد كتب منشورا لأركان سلاح الجو بعنوان «الركائز الأساسية لوسائل حرب المعلومات» Cornerstones of Information Warfare، معرِّفا المصطلح على أنه «أي إجراء من شأنه أن يحجب، أو يستغِل[2]، أو يُتلف، أو يُدمر معلومات العدو ووظائفها» بقصد أساسي هو «تحطيم إرادته أو قدرته القتالية». وعلى سبيل الإيضاح أضاف ويفر، «إن قصف منشأة مبدلات الهاتف هو وسائل حرب معلومات، وكذلك تدمير برمجية تشغيل منشأة مبدلات».

في الأول من أكتوبر، كان السرب 609 قد بدأ العمل، بطاقم يتكون من ثلاثة ضباط فقط، وهم: رودز، وويفر، ومساعد للطاقم، يحتلون غرفة صغيرة في الطابق السفلي بمقر قاعدة «شاو» الجوية، وهي لا تتسع إلا لثلاثة مكاتب فقط، وخط هاتف واحد، وحاسوبين.

في غضون عام، زاد الطاقم إلى ستة وستين ضابطا، كان ثلثهم يعمل على الجانب الهجومي، والباقي كان يعمل في الجانب الدفاعي من المهمة. لكن من حيث الوقت والجهد، فإن النسبة كانت معكوسة – الثلث كان مكرسا للدفاع، والثلثان للهجوم، وكان من يعمل في الجانب الهجومي يوضع في أماكن منفصلة، خلف أبواب مؤصدة بأقفال متداخلة (أقفال ذات أرقام).

في فبراير من العام 1997، عقد السرب أول «تدريب للراية الزرقاء» Blue Flag Exercise[*] كامل. كانت الخطة هي أن يستخدم الطاقم المهاجم وسائل حرب المعلومات للاعتداء على الجناح الجوي لقاعدة «شاو» الجوية، في حين يحاول الطاقم الدفاعي صد الهجوم. سخر أحد ضباط الجناح الجوي من الفرضية، وقال إن جميع اتصالات الجناح مشفرة، ولا أحد يمكنه الدخول إلى هناك.

(*) «تدريب الراية الزرقاء» Blue Flag Exercise هو تدريب للقوات الجوية الأمريكية لتدريب المشاركين على المستوى العملياتي للحرب، ويديره سرب التدريب 505 في «ميدان هورلبورت» Hurlburt Field. [المترجم].

لكن المهاجمين اخترقوا كلمات المرور، واستكشفوا الشبكة، وعثروا على ثغرات نفذوا من خلالها، وحالما صاروا في الداخل استولوا على الشبكة. أصدروا أوامر مزيفة لتخفيف أحمال أسلحة الجناح الجوي، لكي تُلحق الطائرات ضررا أقل بالعدو، وغيروا مسارات وجداول طائرات تزويد الوقود (الطائرات الصهريجية)، التي كان من المفترض أن تزود الطائرات المقاتلة في أثناء الطيران، ونتيجة لذلك ينفد الوقود من الطائرات المقاتلة قبل أن تستطيع القيام بمهماتها.

كانت مناورة مِنضدية، وليست تدريبا حيا. لكن إذا كانت المناورة حقيقية، وإذا فعل خصم في وقت الحرب ما فعله مهاجِمو السرب 609، فستكون خطة حرب سلاح الجو الأمريكي قد تحطمت. ربما يكون بعض الطيارين، وهم ينظرون إلى الأوامر الصادرة لهم، قد أدركوا أن هناك شيئا ما خاطئا، وأجروا تعديلات، لكن من تلك النقطة فصاعدا، لم يكن هؤلاء ولا قادتهم سيعرفون ما إذا كان يمكنهم أن يثقوا بأي أوامر يتلقونها أو أي معلومات يرونها أو يسمعونها. كانوا سيفقدون الثقة بما لديهم من نظم للقيادة والسيطرة.

قرب نهاية المناورة، واتباعا لنص (سيناريو) معلب معد مسبقا، درأ الدفاع الهجوم على نظم معلومات الجناح، وتغلب في المعركة. لكن في الواقع، كان الجميع يعلم أن المناورة كانت هزيمة من الجهة الأخرى. لو لم يكن المهاجمون مُقيَّدين بقواعد المناورة، لكانوا قد أوقفوا تشغيل عمليات الجناح برمتها، تماما مثلما كان تدريب «المتلقي المؤهل» سيكشف بعد بضعة أشهر، وعلى نطاق أوسع هو جيش الولايات المتحدة. أما في هذه الحالة، فإن جناحا حيويا في سلاح الجو كان على نحو مُرَوِّع عُرضة لهجوم بوسائل حرب معلومات، ولم يُمكنه فعل أي شيء حياله.

عرف رودز كيف يوقف تشغيل الجناح الجوي في تدريب «الراية الزرقاء» لأنه حينما كان في الماضي رئيسا لفرع وسائل حرب المعلومات في قيادة القتال الجوي، كان قد استخدم بعض هذه التقنيات في نماذج مُحاكاة لهجمات على أجنحة جوية معادية.

بعد بضعة أشهر من بيان الراية الزرقاء، اندلعت حرب حقيقية، وجعل القادة الجدد لوسائل حرب المعلومات أول مشاركة لهم في القتال، أكثر قدرة وأعلى مرتبة مما قد كانوا عليه في الحرب ضد صدام حسين في بداية العقد.

طوال العام السابق، كانت الولايات المتحدة وحلفاؤها في حلف شمال الأطلسي (ناتو) قد فرضوا إنفاذ «اتفاقيات دايتون» Dayton Accords - معاهدة ديسمبر من العام 1995 التي أنهت الحرب الوحشية للرئيس الصِربي سلوبودان ميلوسيفيتش Slobodan Milosevic في البوسنة والهرسك Bosnia-Herzegovina - من خلال تشكيل أُطلق عليه «قوة تحقيق الاستقرار» (إس فور) Stabilization Force (SFOR)، كانت تطارد أيضا مجرمي الحرب الصرب، وتسعى إلى ضمان حرية ونزاهة انتخابات البلاد، التي كان من المقرر عقدها في سبتمبر من العام 1997.

كان لدى قوة تحقيق الاستقرار جانب أبيض معلن، يتألف من قوات مسلحة نظامية، وجانب أسود سري، يتألف من وحدات عمليات خاصة وجواسيس. كان الجانب الأسود السري يحتاج إلى بعض المساعدة. لم يقمع ميلوسيفيتش مُجرمي الحرب كما كان قد وعد. لذلك، انتهى الأمر إلى أن الوحدة «جيه - 39» J - 39، وحدة «سوب كامبل» فائقة السرية في هيئة الأركان المشتركة بالبنتاغون - من خلال روابط مع وكالة الأمن القومي، وسرب وسائل حرب المعلومات 609، ومركز سلاح الجو لوسائل حرب المعلومات في سان أنطونيو، وغيرها من دوائر الاستخبارات - طورت الأدوات والتقنيات من أجل ما كانوا يرون أنه الوجه الجديد للقتال.

خاضت الوحدة «جيه - 39» أولى مُغامراتها الحربية[3] في 10 يوليو من العام 1997، مع عملية «تانغو» Tango، حيث ادعت فرق الرجال الخمسة من قوات العمليات الخاصة البريطانية أنهم مسؤولون رسميون من الصليب الأحمر، وتمكنوا من القبض على أربعة من أكثر المطلوبين من مجرمي الحرب الصرب. كانت عملية «تانغو» قد سبقتها عمليات استطلاع سرية، تنصتٌ على الهواتف، وتوسيم للسيارات بأجهزة بث لنظام التموضع العالمي (جي بي إس GPS)، وتنصيب كاميرات في بضع مناطق رئيسية داخل أجسام أشياء تبدو مثل الصخور (بدعة من تصميم فنيي استخبارات الجيش الميداني (القوات البرية) في منشأة فورت بيلفوار Fort Belvoir العسكرية بولاية فيرجينيا).

في أوج «قوة تحقيق الاستقرار»، فقد شارك فيها أكثر من ثلاثين ألف جندي من قوات حلف شمال الأطلسي[4]، وهي بكل المقاييس كانت عملية انتشار عالية المستوى، مما استفز المواطنين الصرب للقيام بمظاهرات متكررة ضد وجود الغرب.

سرعان ما أدرك المسؤولون الأمريكيون أن هذه الاحتجاجات كان ينظمها بعض مذيعي إحدى المحطات التلفزيونية المحلية، إذ كانوا يطلبون من المشاهدين الذهاب إلى موقع معين، في وقت محدد، ويلقون الحجارة على الجنود الغربيين.

طلب إيريك شينسيكي Eric Shinseki، جنرال الجيش الميداني (القوات البرية) الأمريكي المسؤول عن قوات حلف شمال الأطلسي في البوسنة، طلب من هيئة الأركان المشتركة – التي بدورها أمرت الوحدة «جيه - 39» – استحداث وسيلة لإيقاف أجهزة البث التلفزيوني حينما تظهر تلك النشرات الإخبارية على الهواء.

كان بعض التقنيين في الوحدة «جيه - 39» من ولاية تكساس، وكانوا يعرفون أجهزة التحكم من بُعد التي كانت تستخدم لإيقاف وتشغيل المضخات في آبار النفط. تعاقدوا مع مُختبرات سانديا Sandia Laboratories، وهي شركة نظم دفاعية عالية التقانة، لتصنيع جهاز مماثل من أجل هذه العملية. في أثناء ذلك، كان محللو قاعدة «كيلي» الجوية يُجرون بعض الحسابات التي أوضحت أن خمسة أبراج تلفزيونية فقط هي التي كانت تبث الإرسال التلفزيوني إلى خمسة وثمانين في المائة من المنازل الصربية. بعض الصرب، الذين كانوا يعملون سرا في القسم الأسود لقوة تحقيق الاستقرار، نصبوا صناديق «سانديا» على تلك الأبراج الخمسة، وحيثما كان يصعب على العملاء تنصيبها على نحو سري خفي، كانوا يخبرون أحد الحراس بأن الصندوق هو مرشح جديد من أجل جودة الفيديو عالية الدقة، وكان الحارس يسمح لهم بالمرور.

حالما جُهِّزت الصناديق، كان المهندسون في مقر «قوة تحقيق الاستقرار» يرصدون محطات التلفزيون. وحينما كان يبدأ أحد مذيعي الأخبار في حث المشاهدين على التظاهر، كانوا يوقفون تشغيل جهاز البث الذي يحمل إشارات تلك القناة.

أيضا، اعتمد المسؤولون الأمريكيون على علاقاتهم مع هوليوود، وأقنعوا بعض منتجي التلفزيون بإمداد إحدى المحطات المحلية الصديقة ببرامج شهيرة ذات شعبية، وفي الساعات التي كانت تجري فيها المظاهرات على نحو متكرر،

(*) «باي واتش» Baywatch هو مسلسل درامي أمريكي عن حراس شاطئ (منقذين) في مقاطعة لوس أنجلوس بولاية كاليفورنيا، يقومون بدوريات في شواطئ لوس أنجلوس، وهو بطولة ديفيد هاسيلهوف David Hasselhoff. كان المسلسل أحد أكثر البرامج التلفزيونية مشاهدة في العالم، واستمر عرضه في الفترة من العام 1989 حتى العام 2001. [المترجم].

كانت المحطة ستذيع حلقات باي واتش Baywatch(*)، أكثر العروض شعبية في العالم. الكثير من الصرب، الذين ربما خلاف ذلك كانوا سيخرجون إلى الشوارع لإثارة المتاعب، بقوا في منازلهم لمشاهدة الفتيات وهن يمرحن مرتديات ملابس السباحة (البكيني).

زار الجنرال شينسيكي المقر لاستعراض بيان عملي لهذه التكنولوجيا. طلب شينسيكي من المهندس الذي كان يرصد المحطات إيقاف تشغيل أحد مواقع البث. نَقَر المهندس أحد مفاتيح التبديل بطرف إصْبَعه، فتوقفت تماما المحطات التي كان يبثها ذلك البرج.

كان شينسيكي مندهشا. وقلب أحد المهندسين، وهو يراقب رد فعل الجنرال، عينيه تعبيرا عن السخط ونفاد الصبر، وهمس إلى أحد زملائه، «بحقك، إنه مفتاح تبديل تشغيل وإيقاف!».

لم تكن هذه هي الخدعة الأكثر تطورا من بين الخدع المثيرة التي كان الفريق قادرا على القيام بها.

بعد مُضي بضعة أشهر، بات من الواضح أن «اتفاقيات دايتون» كانت آخذة في الانهيار. بدأ الجنرال ويسلي كلارك Wesley Clark، قائد حلف شمال الأطلسي، في التخطيط لضربات جوية ضد الأهداف العسكرية الرئيسية لميلوسيفيتش. هيأت الوحدة «جيه39-» الطريق قبل الموعد المقرر بوقت كافٍ.

كانت أولى خطوات أي عملية قصف هي عرقلة أو تعطيل نظام الدفاع الجوي للعدو. اكتشف اثنان من الاختصاصيين - مُعاران من وحدة استخبارات خاصة في ولاية أريزونا Arizona - أن نظام الدفاع الجوي في صربيا يمر عبر نظام الاتصالات المدنية في البلاد.

(أصداء غزو هايتي الذي أُجهض في العام 1993، حينما علم محترفو استخدام برمجية «عفريت الاتصال الهاتفي» في قاعدة «كيلي» الجوية الشيء ذاته عن هايتي، وخططوا لإيقاف تشغيل جهاز الرادار عن طريق إغراق نظام الهاتف بأسره بإشارات انشغال الخط).

كان لدى الوحدة «جيه39-» نصيبها من محترفي استخدام برمجية «عفريت الاتصال الهاتفي» السابقين، وبإذن من وزير الدفاع ويليام كوهين William

Cohen (الذي كان يتعين أخذ موافقته على أي عملية هجومية تنطوي على وسائل حرب معلومات)، اخترقت الوحدة «جيه39-» نظام الهاتف الصربي لتتفحص كل شيء ربما يحتاج إلى معرفته الجنرال كلارك وطاقمه للتخطيط، مثل: كيف كان النظام يعمل، وأين كانت نقاط الضعف والثغرات الأمنية.

تحقق الاختراق بسبب بعض الحظ الجيد الذي أتى في التوقيت الجيد المناسب. أولا، كان مدير وكالة الاستخبارات المركزية جورج تينيت George Tenet قد أنشأ أخيرا وحدة سرية تسمى «مركز عمليات المعلومات (أي أو سي)» Information Operations Center (IOC) ، كان الغرض الرئيسي منها هو إرسال جواسيس لغرس إحدى الأدوات، مثل: أجهزة تنصت، أو قرص مرن، وفي أعوام لاحقة محرك أقراص مصغر (ذاكرة فلاشية)، أو أي شيء آخر قد يتطلبه الأمر. كان هذا سيمكن فرق استخبارات الإشارة (سيجينت) في وكالة الأمن القومي أو أي دائرة أخرى من اعتراض الاتصالات. في هذه الحالة، نصَّب «مركز عمليات المعلومات» أداة في المحطة المركزية لشركة الهاتف الصربية.

البعض الآخر من الحظ كان أن الصرب قد رقَّوا أخيرا برمجيات نظام الهاتف لديهم، والشركة السويسرية التي باعتهم البرمجيات أعطت الرموز الأمنية لاستخبارات الولايات المتحدة.

حالما كانت الطواقم التقنية للوحدة «جيه - 39» قد اخترقت نظام الهاتف الصربي، كان باستطاعتهم التجوال عبر الشبكة بأسرها، بما في ذلك خطوط الدفاع الجوي وخطوط الاتصالات العسكرية الصربية برمتها.

كان ضابط برتبة كولونيل في الجيش الميداني (القوات البرية) الأمريكي يرصد العملية من الخلفية في البنتاغون، وأطلع جون هامري، نائب وزير الدفاع، على ما كان يجري. سأل هامري عن مدى ثقتهم بأن الخطة كانت ستؤدي إلى إحباط القادة الصرب.

أجاب الكولونيل: «بناء على خبرتي بوصفي قائد كتيبة، إذا التقطتَ سماعة الهاتف ولم تستطع سماع أحد أو التحدث إلى أي أحد، فإن هذا الأمر محبط جدا».

قال هامري: «هذا جيد بما فيه الكفاية بالنسبة إليَّ».

بدأ الجنرال كلارك حملة القصف في 24 مارس 1999. لم يكن قادة سلاح الجو يثقون بمخطط خداع أجهزة الرادار، وفي المقابل أمروا الطيارين بالتحليق على

ارتفاعات عالية جدا، على الأقل خمسة عشر ألف قدم، بعيدا عن مدى الصواريخ الصربية المضادة للطائرات. لكن في بعض الحالات التي كانت طائرات التحالف تنخفض، كان رجال العمليات في الوحدة «جيه - 39» يخترقون نظام الدفاع الجوي كما هو مخطط، ويعملون على تغذيته بمعلومات مزيفة، مما جعل راصدي شاشة الرادار يعتقدون أن الطائرات كانت آتية من جهة الغرب، في حين أنها في الواقع كانت آتية من جهة الشمال الغربي.

كان يتعيَّن أن يكون الخداع ماكرا وغير ملحوظ. وكان ينبغي إيقاف تشغيل جهاز الرادار فترة وجيزة، بما يكفي لجعل الضباط الصرب يلقون باللوم على الخلل الميكانيكي، وليس فترة طويلة بالقدر الذي يجعلهم يشتبهون في وجود تخريب، الحالة التي ربما يتحولون فيها من التوجيه التلقائي (المؤلل) إلى التحكم اليدوي. (على مدار الحرب، تمكن الصرب من إسقاط طائرتين، طائرة من طراز «إف - 16» ومقاتلة شبح (الطائرة الخفية) من طراز «إف - 117»، تحديدا حينما أجرى أحد الضباط هذا التحويل). بخلاف ذلك، استمرت فرق الدفاع الجوي مصوبة أسلحتها تجاه مساحات كبيرة من السماء لم تكن تحلق فيها طائرات.

كان لحملة الوحدة «جيه - 39» هدف آخر هو دق إسفين للتفرقة بين قوات ميلوسيفيتش شبه العسكرية المعروفة باسم «إم يو بي» (MUP) والجيش اليوغوسلافي النظامي (ڤي جيه VJ). كانت وكالة الأمن القومي قد حصلت على أرقام هاتف وفاكس بعض الضباط في كلتا المؤسستين. أرسل ضباط الوحدة «جيه-39» رسائل إلى قادة الجيش اليوغوسلافي النظامي، معربين عن إعجابهم بما يتمتعون به من احترافية في الدفاع عن الشعب اليوغوسلافي، ولحثهم على البقاء غير مسيسين. في مرحلة ما، قصف الجنرال كلارك مقر قوات ميلوسيفيتش شبه العسكرية، وكذلك مقر الجيش اليوغوسلافي النظامي في وقت واحد تقريبا، وبينما كانت الطائرات تحلق في الجو، أرسلت الوحدة «جيه - 39» رسالة إلى قادة الجيش اليوغوسلافي النظامي، محذرة إياهم من مغادرة البناية. بعد تدمير المقرين، سمع الناجون من قوات ميلوسيفيتش شبه العسكرية – كان بعضهم مصابا، وجميعهم مرتعبون - أن ضباط الجيش اليوغوسلافي النظامي لاذوا بالفرار من مقارهم سالمين مبكرا قبل القصف بزمن، وبذلك بدأ الشك يساورهم في أن الجيش اليوغوسلافي النظامي كان يتعاون

مع حلف الناتو. مزق انعدام الثقة الجانبين إربا كلا على حدة، تماما مثلما استهدفت الوحدة «جيه - 39».

بينما كان رجال العمليات في الوحدة «جيه - 39» يتوغلون بعمق داخل منظومة القيادة والسيطرة الخاصة بالجيش الصربي، بدأوا في اعتراض الاتصالات بين ميلوسيفيتش وأتباعه المقربين، وكان الكثير منهم من المدنيين غير العسكريين. مجددا، وبمساعدة وكالة الأمن القومي، رسم جنود المعلومات خريطة هذه الشبكة الاجتماعية، وحصلوا على أقصى ما يمكن معرفته بشأن الأتباع المقربين أنفسهم، بما في ذلك أرصدتهم المالية، وأعدوا خطة لتجميد أصول أتباع ميلوسيفيتش، كإحدى وسائل الضغط عليه وعزله عن قاعدة نفوذه.

اعترض محامو البنتاغون على الاقتراح، هم في الواقع كانوا ينبذون بشدة أي خطة تمس المدنيين الصرب. لكن بعد ذلك، وفي أثناء عطلة نهاية الأسبوع في 17 أبريل، نُظم ماراثون بلجراد Belgrade، الذي كان فيه عداؤو سباق 26.2 ميل سيعبرون مرتين جسرا كان هدفا مهما في حملة القصف. وعلى أثير الموجات الإذاعية المحلية والدولية، وصفت السلطات الصربية هذا الحدث بأنه احتجاج جريء يتحدى حرب «الناتو» الجوية، وهو برهان على الضعف الخسيس للغرب في مواجهة شجاعة الشعب الصربي وولائه للرئيس ميلوسيفيتش.

كان الرئيس كلينتون يشاهد البث التلفزيوني لسباق الماراثون وهو في حالة مزاجية سيئة. في يوم الإثنين الذي سبق، كان قاضٍ فدرالي قد رأى أن الرئيس أهان المحكمة بإدلائه بشهادة «كاذبة عمدا» بشأن علاقاته مع متدربة البيت الأبيض مونيكا لوينسكي Monica Lewinsky. والآن هذا! كان ويس كلارك قد عاهده بأن ميلوسيفيتش سيسقط بعد بضعة أيام من القصف، لكن أربعة أسابيع مرت، وكان الوغد يحتقر العالم الغربي.

أرسل كلينتون خطابا لتكثيف الضغط؛ وعلى نحو مفاجئ، سحب محامو البنتاغون اعتراضاتهم على ملاحقة أتباع ميلوسيفيتش؛ وفي يوم الإثنين التالي، بدأت الوحدة «جيه - 39» المرحلة التالية من العمليات(*).

(*) أيضا توصلت الوحدة «جيه - 39» إلى كيفية اختراق حسابات ميلوسيفيتش المصرفية الخاصة، وكان الرئيس كلينتون مفتونا بالفكرة. لكن كبار المسؤولين، لاسيما في وزارة الخزانة، نصحوا بشدة بعدم المضي في هذا الطريق، محذرين من نتائج عكسية خطيرة. في الأعوام اللاحقة، تتبعت دوائر الاستخبارات الأمور المالية لزعماء معادين آخرين، لكن خيار الاختراق الفعلي لحساباتهم المصرفية لم يكن هناك مطلقا سعي حثيث لتنفيذه. [المترجم].

كان أحد كبار المانحين السياسيين للرئيس ميلوسيفيتش يمتلك منجما للنحاس. أرسلت الوحدة «جيه - 39» إليه خطابا، محذرة من أن المنجم سيُقصف إذا لم يتوقف عن دعم الرئيس الصربي. لم يستجب المانح. لم يمض وقت طويل حتى كان أحد مقاولي (متعهدي) وكالة الاستخبارات المركزية الأمريكية قد اخترع جهازا مصنوعا من جدائل طويلة من ألياف كربونية، تؤدي إلى حدوث دائرة قصر (ماس كهربائي) عندما تلامس سلكا كهربائيا. حلَّقت طائرة مقاتلة أمريكية فوق منجم النحاس، وأسقطت ألياف الكربون فوق خط نقل الطاقة الكهربائية الخاص بالمنجم، وقطعت عنه الكهرباء. كان الإصلاح سريعا وسهلا، ولكن كذلك كان مغزى الرسالة أيضا. تلقى المانح خطابا آخر، ذكر فيه أن انقطاع التيار الكهربائي كان بمنزلة تحذير، وإذا لم يغير أساليبه، فستسقط القنابل. على الفور قطع اتصالاته مع ميلوسيفيتش.

صعّدت الوحدة «جيه - 39» حملتها لإغلاق آلة ميلوسيفيتش الدعائية. كانت إحدى شركات الأقمار الاصطناعية الأوروبية هي التي تحمل بث إرسال بعض المحطات الموالية للرئيس ميلوسيفيتش. زار مسؤول رفيع المستوى في قيادة الولايات المتحدة في أوروبا رئيس الشركة وقال له إن 80 في المائة من أعضاء مجلس إدارته هم من دول حلف شمال الأطلسي (ناتو)؛ وحينما أخبره رئيس الشركة كم كانت تدفع له المحطات الصربية، عرض الضابط الأمريكي دفع نصف مليون دولار إضافية إذا أغلقها، فامتثل رئيس الشركة.

في تلك الأثناء، كانت دوائر استخبارات الولايات المتحدة قد اكتشفت أن أبناء ميلوسيفيتش يقضون عطلتهم في اليونان. التقط الجواسيس صورا لهم وهم مستلقون على الشاطئ. بعد إحدى عمليات القصف التي سببت انقطاع التيار الكهربائي في بلغراد، ألقت الطائرات الأمريكية منشورات بها صور فوتوغرافية تحت عنوان حماسي مُدوٍ أن ميلوسيفيتش أرسل أولاده للاستمتاع بحمام شمسي في اليونان في حين كان شعبه يجلس في الظلام.

في النهاية، أطلقت الوحدة «جيه - 39» حملة لإزعاج ميلوسيفيتش ومن حوله. اتصلوا بهاتفه المنزلي مرارا وتكرارا، ليلا ونهارا، وحينما كان يلتقط أحد سماعة الهاتف ليرد، كانوا يصمتون ولا يقولون شيئا. كان النظير البريطاني لوكالة الأمن القومي – مقر الاتصالات الحكومية (جي سي إتش كيو)Government

Communications Headquarters (GCHQ) - يرصد المكالمات وعمموا تسجيلات صوتية لزوجة ميلوسيفيتش وهي تسب وتلعن وتصفع الهاتف. على نحو مرح، أخبر أحد أعضاء مقر الاتصالات الحكومية نظيره الأمريكي، «إن الأمر يحلو لنا حينما يتحدثون إلينا بفحش».

كذلك، كانت الوحدة تهاتف جنرالات ميلوسيفيتش على هواتفهم المنزلية، وكانت تشغِّل تسجيلا صوتيا لشخص كان يُعرِّف نفسه على أنه الجنرال كلارك، سائلا ببشاشة، وبلسان صربوكرواتي (سلافي) طلق: كيف تسير الأمور؟ ويحثهم على وقف القتال.

في 4 يونيو استسلم ميلوسيفيتش. كان ملحوظا على نطاق واسع أنه لم يكن أحد من قبل مطلقا قد كسب حربا بالقوة الجوية وحدها. لكن هذه الحرب أيضا لم يكن الفوز بها على هذا النحو. كان الفوز بها من خلال مزيج من الدك بالضربات الجوية وأثر عزلة وسائل حرب المعلومات.

بعد ذلك، في إحاطة ما بعد الحرب، أشاد الأدميرال جيمس إيليس James Ellis، قائد قوات التحالف في جنوب أوروبا، بعملية المعلومات، ووصفها بأنها «في آن واحد نجاح كبير[5]... وربما تكون الإخفاق الكبير للحرب». كانت جميع الوسائل مهيأة، واستطرد قائلا: لكن «لم يُستخدَم سوى بضع منها». لقد وظفت الحملة «أناسا رائعين» مع «تواصل رائع مع القيادة»، لكنهم لم يكونوا في تكامل مع قيادات العمليات؛ لذلك، فقد كان تأثيرهم «في التخطيط والتنفيذ» أقل مما ربما كان لديهم. كتب إيليس أن مشروع وسائل حرب المعلومات برمته كان يتمتع بـ «إمكانات مذهلة» وينبغي أن يصير هدف الجهد الرئيسي في الحروب غير المتكافئة المقبلة. مع ذلك، فإن مفهومها «لم يكن المقاتلون قد استوعبوه بعد». وأحد أسباب هذا التردي، كما قال، هو أن كل شيء بشأن وسائل حرب المعلومات كان «سريا جدا وخارج نطاق وصولهم إليه»، ويتطلب تصاريح أمنية خاصة لا يمتلكها سوى بضعة ضباط. خلص إيليس إلى أنه إذا كان قد استُغِلت الأدوات والتقنيات بشكل كامل، فربما كانت الحرب ستستغرق نصف المدة.

كان هذا هو الجانب الأكثر وضوحا في حملة وسائل حرب المعلومات، إذ إن التخطيط لها وتنفيذها كان يجري بواسطة وحدة سرية تتبع هيئة الأركان المشتركة

في البنتاغون، بمعاونة جهات أكثر سرية وكتمانا، وهي: وكالة الأمن القومي، ووكالة الاستخبارات المركزية، ومقر الاتصالات الحكومية. بينما كان القرن العشرون يوشك على الانتهاء، لم يكن القادة العسكريون الأمريكيون راضين عن اضطلاع المخترقين قراصنة الحاسوب بأعمال الجنود وقاذفي القنابل. كان بضعة من كبار الضباط منصاعين للتجريب، لكن وزارة الدفاع كانت تفتقر إلى الأفراد أو الإجراءات (البروتوكولات) لدمج هذا البعد الجديد للحرب في خطة معركة فعلية. كان كبار الجنرالات قد وقَّعوا على وثائق تنظيمية بشأن «وسائل حرب المعلومات» (وقبل ذلك، «الحرب المضادة للقيادة والسيطرة»)، لكن يبدو أنهم لم يأخذوا الفكرة على محمل الجد.

ثمة مجموعة صغيرة من الجواسيس والضباط هي التي أقدمت على تغيير ذلك.

8

الولوج المُصَمَّم وفقا للحاجة

كان آرت موني ART MONEY حائِرا مُشَوَّشا. كان موني هو مساعد وزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات إيه إس دي(سي3آي) ASD(C3I)، ومن ثم هو رجل البنتاغون المسؤول عن وسائل حرب المعلومات، واتصاله المدني (غير العسكري) مع وكالة الأمن القومي. كان ينبغي أن تكون الأعوام القليلة الفائتة قد بررت حماسته. إن مناورة تدريب «المُتَلَقِّي المُؤَهَّل»، وتحقيقات «الشروق الشمسي»، وعملية «مَتَاهَة ضوء القمر» كانت قد أنجبت وعيا بأن شبكات الحاسوب العسكرية غير حصينة وعُرضة للهجوم. أثبتت عمليات الوحدة «جيه - 39» في البلقان أنه كان يمكن استغلال أوجه الضعف والثغرات الأمنية في شبكات الدول الأخرى من أجل تحقيق

«كان المغزى من استخبارات الإشارة، المهمةِ الرئيسية لوكالة الأمن القومي، هو جمعَ المعلومات الاستخباراتية عن طريق النفاذ إلى اتصالات العدو»

مكاسب عسكرية، إذ إن معرفة كيفية استغلالها كان من الممكن أن تمنح الولايات المتحدة تفوقا في وقت الحرب. مع ذلك، لم يبد أدنى الاهتمام بإمكانات التكنولوجيا سوى عدد من كبار ضباط أمريكا.

يرجع اهتمام موني بالتكنولوجيا العسكرية إلى إحدى ليالي العام 1957، حينما كان ساهرا على حراسة إحدى قواعد الجيش الميداني (القوات البرية) في كاليفورنيا California، ونظر إلى السماء ورأى القمر الاصطناعي الثاني للاتحاد السوفييتي «سبوتنيك 2» Sputnik II وهو يدور حول الأرض، قبل أن يطلق الأمريكيون أول أقمارهم الاصطناعية، كان استشرافا للمستقبل، مُفزعا ومُخيفا وآسرا وجذابا في آن واحد. بعد مُضي أربعة أعوام التحق موني بجامعة سان هوزيه (سان خوسيه) الحكومية San Jose State للحصول على درجة علمية في الهندسة. كانت مُنشأة لوكهيد Lockheed في مدينة سانيفال Sunnyvale المجاورة تَوَّاقة إلى توظيف أي مهندس. حصل موني على وظيفة في نوبة الليل، مُساعدا في بناء النظام الذي كان سيطلق صاروخ بولاريس Polaris الجديد من أنبوب في إحدى الغواصات، وسرعان ما عمل موني على أقمار تجسس اصطناعية سرية جدا. وبعد حصوله على دبلوم الدراسات العليا، عمل على الأجهزة السرية للغاية التي كانت تُستخدَم لاعتراض الإشارات الراديوية (اللاسلكية) الصادرة عن اختبارات الصواريخ السوفييتية.

من لوكهيد، انتقل موني للعمل في شركة «إي إس إل» ESL، الشركة التي كان بيل بيري قد أسسها لبناء وتطوير مُعدات استخبارات الإشارة (سيجينت) لوكالة الأمن القومي ووكالة الاستخبارات المركزية. بحلول العام 1990 ارتقى موني إلى أن أصبح رئيسا للشركة. بعد مُضي ستة أعوام، وبإلحاح من بيري، مُرشده القديم ومُعلمه منذ فترة طويلة، الذي أصبح وزيرا للدفاع، جاء موني للعمل في البنتاغون، مساعدا لوزير سلاح الجو لشؤون البحث والتطوير والازدياد (التعزيزات).

وضعته هذه الوظيفة في اتصال متواتر مع جون هامري John Hamre، المراقب المالي للبنتاغون. في فبراير من العام 1998، حينما اندلع هجوم «الشروق الشمسي»، كان هامري يشغل منصب نائب وزير الدفاع، وأدرك بوعيه أنه لا أحد ممن حوله كان يعرف ماذا يفعل. من ثم أقنع رئيسه، وزير الدفاع وليام كوهين William

Cohen، بتعيين آرت موني مساعدا جديدا لوزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات إيه إس دي(سي3آي).

كان موني موهوبا بالفطرة وملائما للمهمة. كان هامري ينوي وضع الأمن السيبراني على رأس الأولويات. أصبح موني كبير مستشاريه للشؤون السيبرانية، وهو كان أحد مسؤولي البنتاغون الأفضل اطلاعا على القضايا السيبرانية، وأكثر المسؤولين الرسميين اتصالا بهذا الشأن. كان موني هو الذي اقترح تنصيب أنظمة كشف التسلل على حواسيب وزارة الدفاع، وهو الذي جلب داستي رودز إلى الوحدة «جيه - 39» بعد أن سمع بما قام به من عمل في مناورات الراية الزرقاء في السرب 609 لوسائل حرب المعلومات، وكان هو الذي جمع بين جهود الوحدة «جيه - 39» ووكالة الأمن القومي، ووكالة الاستخبارات المركزية في أثناء حملة البلقان.

عند هذه النقطة، كان ينبغي أن يكون مفهوم وسائل حرب المعلومات - أو وسائل الحرب السيبرانية، كما كانت تُسمى حينئذ - قد شهد طفرة، لكن لم يكن ذلك قد حدث، لأن معظم كبار الجنرالات كان لايزال غير مهتم، أو في بعض الحالات مُنَاهِضا.

في صيف العام 1988[1]، في أعقاب «الشروق الشمسي»، كان لموني دور محوري فاعل في تأسيس فريق العمل المُشتَرَك لحماية شبكات الحاسوب (جيه تي إف-سي إن دي)، باعتباره مكتبا لتنسيق تدابير وقائية لكل أنظمة الحاسوب في وزارة الدفاع، بمن في ذلك طواقم العمل لمركز إنذار يعمل على مدار الساعة وطوال أيام الأسبوع (7/24)، وإعداد مُسَوَّدة إجراءات (بروتوكولات) تبين تفاصيل ما ينبغي فعله في حالة وقوع هجوم. باختصار، كان موني يعمل على تجميع إجابة السؤال الذي طرحه هامري في بداية تحقيقات «الشروق الشمسي»، من الذي يتولى زمام الأمور؟

كانت الخطة المبدئية هي أن يكون فريق العمل المُشتَرَك لحماية شبكات الحاسوب (جيه تي إف-سي إن دي) منوطا بدور هجومي أيضا، هو مهمة تطوير واستحداث بدائل لمهاجمة شبكات الخصم. أقام داستي رودز بؤرة استيطانية سرية صغيرة مُخصصة للقيام بذلك فقط. لكن موني، وسوب كامبل، الجنرال ذا النجمة الواحدة المسؤول عن فريق العمل، كانا يعرفان أن فروع القوات المسلحة لم تكن لتمنح مثل هذه الصلاحيات لمكتب صغير بلا سُلطة قيادية.

مع ذلك، شدد كامبل على أنه، على أقل تقدير، ينبغي إحاطة فريق العمل علما في حالة ما إذا كان لدى الفروع العسكرية خطط أو برامج لعمليات هجومية سيبرانية (وكان كامبل يعلم أن الفروع لديها). كانت حُجته غير قابلة للجدال، كان محللو فريق العمل في حاجة إلى تطوير واستحداث دفاعات لصد الهجمات السيبرانية، ومعرفة ما هي أنواع الهجمات التي كان جيش الولايات المتحدة قد ابتكرها، لأهمية ذلك في مساعدتهم على توسيع نطاق الدفاعات، لأنه أيا كانت الإجراءات التي ستتخذها أمريكا ضد خصومها، فمن المحتمل أن خصومها كانوا قريبا سيُدبرون مثلها ضد أمريكا.

اقتنع كوهين بالحُجَّة، وكتب مذكرة إلى قادة الفروع، آمرا إياهم بتَشَارُك ما لديهم من خطط مُهاجمة شبكة الحاسوب (سي إن أيه) مع فريق العمل المُشتَرَك. مع ذلك، في اجتماع ترأسه جون هامري، تحدث نواب قادة الجيش الميداني (القوات البرية)، وسلاح البحرية، وسلاح الجو نيابة عن رؤسائهم، ونسفوا الأمر الصادر إليهم؛ إنهم لم يعصوا الأمر صراحة، كان هذا سيُعَد تمردا، وهو مخالفة تستوجب الفصل. بدلا من ذلك، أعادوا تعريف خططهم الهجومية على أنها شيء آخر، بذلك كان يُمكنهم ادعاء أنهم لم يكن لديهم مثل هذه الخطط للإخطار بها. لكن مراوغتهم وتملصهم كانا جليين، إنهم فقط لا يرغبون في تَشَارُك تلك الأسرار مع آخرين، حتى إن كان وزير الدفاع هو الذي طلب منهم أن يفعلوا ذلك.

كان جليا أن فريق العمل في حاجة إلى ميثاق أشمل وأوسع نطاقا، وفي حاجة إلى منزلة تتمتع بمزيد من السلطة. لذلك، في 1 أبريل من العام 2000، استُبدِلت كلمة «عمليات» بكلمة «حماية»، وأصبح «فريق العمل المُشتَرَك لحماية شبكات الحاسوب» (جيه تي إف-سي إن دي JTF-CND) يُسمى «فريق العمل المُشتَرَك لعمليات شبكات الحاسوب» (جيه تي إف-سي إن أوو JTF-CNO). كانت تلك العمليات تتضمن ليس فقط حماية شبكات الحاسوب، ولكن، وعلى نحو صريح، تتضمن أيضا مُهاجمة شبكات الحاسب. وُضِع فريق العمل الجديد في نطاق سُلطة القيادة الفضائية للولايات المتحدة U.S. Space Command في مدينة كولورادو سبرينغز Colorado Springs. كان هذا موضعا شاذا غريبا، لكن لم تقبل المهمة أي وحدة سوى القيادة الفضائية (سباسكوم SpaceCom). على أي حال، هي كانت قيادة مُخَوَّلة بممارسة سلطات تخطيط الحرب والتصدي لها.

مع ذلك، كان موني، وكامبل، وهامري، وقائد فريق العمل الجديد، الميجور جنرال (لواء) جيمس دي براين James D. Bryan يرون هذا أيضا ترتيبا مؤقتا. كانت كولورادو سبرينغز بعيدة عن البنتاغون أو أي مركز سلطة آخر. وكان عُشاق الحاسوب (مهووسو الحاسوب) من فريق العمل يشتكون من أن نظراءهم في القيادة الفضائية الذين كان يتعين تداخلهم في المهمة، لم تكن لديهم أي معرفة بشأن الهجوم السيبراني.

كان موني يشعر بأن المهام السيبرانية - خاصة تلك التي تتناول الهجوم السيبراني - في نهاية المطاف كان ينبغي نقلها إلى مقر وكالة الأمن القومي الرئيسي في فورت ميد، وهذا ما فعله ليوتينانت جنرال (الفريق) مايكل هايدن Michael Hayden، المدير الجديد لوكالة الأمن القومي.

جاء مايك هايدن إلى وكالة الأمن القومي في مارس من العام 1999، خلفا لكين مينيهان. لم تكن هذه هي المرة الأولى التي يتبع فيها هايدن خُطى مينيهان. طوال ما يقرب من العامين، ابتداء من يناير من العام 1996، كان هايدن قائدا لقاعدة كيلي الجوية في سان أنطونيو، حيث كان مينيهان قد أدار مركز سلاح الجو لوسائل حرب المعلومات، الذي كان رائدا لكثير مما أُطلق عليه لاحقا وسائل الحرب السيبرانية - هجوما ودفاعا، وفي الوقت الذي وصل فيه هايدن، كان المركز قد ازداد تطورا ومكانة.

لم يكن هايدن قبل توليه منصبه في قاعدة كيلي الجوية يعرف سوى القليل بشأن هذا الموضوع، لكنه سرعان ما أدرك إمكاناته وبوصفه منهجي التفكير يهوى تصنيف الأفكار في فئات، فقد توصل إلى تصور لمهمة أطلق عليها اسم «جي إي دي آيه» GEDA[3] - وهو اختصار لـ: اجلب Gain (اجمع المعلومات)، واستغل Exploit (استخدم المعلومات للنفاذ إلى شبكات العدو)، ودافع Defend (امنع العدو من النفاذ إلى شبكاتنا)، وهاجِم Attack (لا يقتصر الأمر على النفاذ إلى شبكة العدو – عطِّلها، أو أربكها، أو دمِّرها).

للوهلة الأولى، كان التصور يبدو واضحا. لكن كان هدف هايدن الأكثر عمقا هو أن تكون كل هذه المهام متداخلة ومَجدُولة معا، إنها جميعا تشتمل على التكنولوجيا ذاتها، والشبكات ذاتها، والإجراءات والأعمال ذاتها. إن الاستخبارات

والعمليات في الفضاء السيبراني - الأمن السيبراني، والتجسس السيبراني، والحرب السيبرانية - هي مترادفات من حيث الجوهر الأساسي.

كان هايدن مُتمركزا خارج البلاد، رئيسا لاستخبارات قوات الولايات المتحدة في كوريا الجنوبية، حينما سببت هجمات «الشروق الشمسي» و«مَتَاهَة ضوء القمر» إثارة حالة من الذعر لدى كبار المسؤولين، وأدت إلى نتيجة مفادها أن هناك على الأقل بضعة جنرالات أدركوا أن الحديث العصري الشائع بشأن وسائل حرب المعلومات ربما يستحق الاهتمام. على نحو مفاجئ، ومن دون سابق إنذار، وإن لم يكن ذلك إلا من أجل دعم مطالبهم[4] في معارك الموازنة المقبلة، رفع كل فرع من هذه الفروع المسلحة لافتة سيبرانية: نشاط وسائل حرب المعلومات البرية بالجيش الميداني (القوات البرية)، ونشاط وسائل حرب المعلومات البحرية بسلاح البحرية، وحتى وحدة حماية شبكات الحاسوب بسلاح مُشاة البحرية، وانضمت إلى مركز سلاح الجو لوسائل حرب معلومات القائم في المؤسسة العسكرية منذ أمد طويل.

كان الكثير من تلك الكيانات قد نشأ في أثناء فترة ولاية كين مينيهان مديرا لوكالة الأمن القومي، وجعله هذا الاتجاه يشعر بالقلق لثلاثة أسباب: أولا، كانت هناك اعتبارات مالية، إذ إنه كان يُجري خفضا لموازنة الدفاع في أعقاب الحرب الباردة، وكانت حصة وكالة الأمن القومي تُعاني مزيدا من الانخفاض، وهو لم يكن في حاجة إلى كيانات أخرى تُركِّز اهتمامها على مجال ضيق، وتستنزف ما لديه من موارد على نحو أكبر، وهم مُبتدئون في حقل كانت وكالة الأمن القومي قد ابتدعته وأتقنته. ثانيا، كان الأمن العملياتي رديئا لدى بعض هؤلاء المُحاربين السيبرانيين الطموحين، وكانوا عُرضة للقرصنة والاختراق من الخصوم، فإذا اقتحم أحد الخصوم شبكاتهم، ربما يتمكن من الوصول إلى الملفات التي كانت وكالة الأمن القومي قد تشاركتها معهم.

أخيرا، كان هناك قلق على وجود الوكالة ذاته. حينما صار مينيهان مديرا لوكالة الأمن القومي، قال له بيل بيري: كين، عليك أن تُحافظ على غموض «فورت ميد». الغموض، كان هذا هو مفتاح المكان، وأدرك مينيهان مُبكرا أن هذا هو ما هيمن على الرؤساء، ومجلس الوزراء، ورؤساء اللجان، وفرق من المحامين الحكوميين، وقادهم إلى أن يَدَعوا وكالة الأمن القومي تعمل في سرية شبه تامة، وبقدر من الاستقلالية

أكثر من دوائر الاستخبارات الأخرى. كانت مُنشأة فورت ميد العسكرية حيث كان صانعو وكاسرو الشفرات البارعون غير المعروفين يفعلون أشياء كان أشخاص من خارج فورت ميد يمكنهم أن يزعموا أنهم يفهمونها، فضلا على تكرارها وعمل مثلها. وطوال حقبة ما بعد الحرب العالمية الثانية بكاملها تقريبا، فإنهم كانوا قد أدوا دورا عظيما في الحفاظ على السلام، وإن كان هذا غالبا غير معلن.

حينذاك، كان الغموض يتكَشّف وينهار. مع انتهاء الحرب الباردة، اجتث مينيهان المجموعة «أ» الأسطورية، المتخصصة في الشؤون السوفييتية، من أجل تكريس المزيد من الموارد لمواجهة التهديدات الناشئة، بمن في ذلك الأنظمة المارقة والإرهابيون. مع ذلك، كان يمكن أن تظل الوكالة تتباهى بقاعدتها التقنية الأساسية، اختصاصيي التشفير، ومُختبراتها الداخلية، وشراكاتها الفريدة مع المقاولين (المتعهدين) الخارجيين المستترين، حيث كان لايزال الغموض مُتوهجا مُتقدا. كان مينيهان في حاجة إلى بناء تلك القاعدة، وتوسيع نطاقها، وتغيير برنامج عملها، والحفاظ على براعتها وتفوقها، وعدم السماح بإضعافها بفعل الطامحين الأقل شأنا المحبين للشهرة، الذين ينثرون الماء في الجدول نفسه.

في خضم كثرة الكيانات التي كانت تُطالب بقطعة من مضمار كان يوما حكرا على فورت ميد، وما صاحب ذلك من غزارة في المصطلحات المماثلة لما كان في الأساس هو النشاط نفسه (وسائل حرب المعلومات، وعمليات المعلومات، ووسائل الحرب السيبرانية، وما إلى ذلك)، حاول مينيهان أن يرسم خطا ليضع حدا لهذا. في كثير من الأحيان، كان مينيهان يقول لرؤسائه السياسيين: أنا لا أهتم بالاسم الذي تطلقونه عليها، أنا لا أريد شيئا إلا أن تتصلوا بي.

ومن أجل الحفاظ على وكالة الأمن القومي في مركز هذا العالم[5]، أنشأ مينيهان في فورت ميد مكتبا جديدا يُسمى «مركز تكنولوجيا عمليات المعلومات» (آي أوو تي سي) Information Operations Technology Center (IOTC) . كانت الفكرة هي توحيد جميع حوانيت السيبرانية العسكرية المتفرقة، وليس تدميرها، لم يكن مينيهان يرغب في إطلاق حروب بيروقراطية، لكنه رغب في أن يسوقها إلى داخل ولايته.

لم تكن لدى مينيهان السلطة القانونية ولا السطوة السياسية لفعل ذلك عن طريق مرسوم، لذلك استعان بآرت موني، الذي كان قد عرفه طوال أعوام، والذي

كان قد صار من فوره مساعدا لوزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات «إيه إس دي(سي3آي)»، وطلب منه أن يمشِّط موازنات السيبرانية التي تخص الفروع كلٌّ على حدة بحثا عن برامج تتسم بالازدواجية، ولا غرابة في أن موني وجد الكثير منها. أخذ موني ما اكتشفه وذهب إلى جون هامري، وأبرز التكرار الزائد الذي لا لزوم له، وحقق بُغية هامري. قال موني إنه لا توجد دائرة تستطيع أن تؤدي تلك المهام على نحو أفضل من وكالة الأمن القومي، التي تصادف أن لديها مكتبا يُسمى «مركز تكنولوجيا عمليات المعلومات»، وهو مكتب سيكون مثاليا لمواءمة وتنسيق هذه الجهود المتباعدة. كان هامري قد اقتنع أخيرا بقيمة وكالة الأمن القومي، فوافق على الفكرة، ووضع المركز الجديد تحت إشراف موني.

عندما تولى هايدن مسؤولية وكالة الأمن القومي، ضغط عليه موني ليأخذ المركز في اتجاه مختلف. حينما تأسس مركز تكنولوجيا عمليات المعلومات، كان هدف مينيهان هو التأكيد على التكنولوجيا التي كانت الميزة الرئيسية لوكالة الأمن القومي، والمُسوغ المنطقي لبقائها متربعة على قمة الهرم. كان موني يرغب في التشديد على العمليات، وفي استخدام مركز تكنولوجيا عمليات المعلومات على أنه باب خلفي تستطيع وكالة الأمن القومي الدخول منه إلى العمليات السيبرانية الهجومية.

أثارت الفكرة الجدل على عدة أصعدة. أولا، في داخل وكالة الأمن القومي، لم تكن الفكرة تروق للعديد من قدامى الوكالة. كان المغزى من استخبارات الإشارة (سيجينت)، المُهمة الرئيسية لوكالة الأمن القومي، هو جمع المعلومات الاستخباراتية عن طريق النفاذ إلى اتصالات العدو، فإذا هاجمت وكالة الأمن القومي مصدر تلك الاتصالات، كانت الاستخبارات ستنكشف، وكان العدو سيعلم أننا نجحنا في النفاذ إلى شبكته، وكان سيعمل على تغيير رموز شفرته، ويُنقِّح أمنه.

ثانيا، لم تكن فكرة موني مشروعة تماما. بوجه عام، كان الجيش يعمل تحت الباب العاشر من القوانين الفدرالية، في حين كانت دوائر الاستخبارات، بما في ذلك وكالة الأمن القومي، تندرج تحت الباب الخمسين. كان الباب العاشر يسمح باستخدام القوة، في حين أن الباب الخمسين لم يكن يسمح بذلك. كان الجيش يستطيع استخدام المعلومات الاستخباراتية التي كانت تجمعها الدوائر التي تعمل

وفقا للباب الخمسين على أنها ركيزة للهجوم، ولم تكن وكالة الأمن القومي تستطيع شن هجمات من تلقاء نفسها.

ظن موني وهايدن أنه كان يمكن تقديم حجم وإبداء أسباب وجيهة ليتحايل مركز تكنولوجيا عمليات المعلومات على تلك القيود، مثل أنه كان على نحو رسمي يأتمر من وزير الدفاع. لكن الدغل القانوني كان كثيفا جدا لمثل هذا الالتفاف المؤقت البسيط. كان كل فرع من الفروع العسكرية، وربما دوائر أخرى، ستكون له حصة في أي عمل يضطلع به مركز تكنولوجيا عمليات المعلومات، تماما مثل وكالة الاستخبارات المركزية. إنه كان كيانا متداعيا منذ البداية، كان منطقيا من وجهة نظر تقنية بحتة. ومثلما أدرك مينيهان وهايدن، من واقع منصبيهما في مركز سلاح الجو لوسائل حرب المعلومات في سان أنطونيو، فإن مُهاجمة شبكة الحاسوب وحمايتها هما سيان من الناحية العملياتية (التشغيلية)، لكن الصلاحيات القانونية كانت مختلفة ومستقلة.

كان هايدن يعتبر أن مركز تكنولوجيا عمليات المعلومات هو ترتيب جيد بما فيه الكفاية في الوقت الراهن، إنه على الأقل حمى سيادة وكالة الأمن القومي على ميدان السيبرانية، مثلما كان مينيهان قد استهدف. كان سينبغي التريث وتأجيل توسيع نطاقه على المدى الطويل. في تلك الأثناء، كان هايدن - تقريبا منذ لحظة توليه منصبه - يواجه مُستنقعا من مشكلات صعبة أخرى.

بُعَيد وصول مينيهان إلى فورت ميد، سمع إشاعات بشأن تقرير سري جدا بعنوان «هل نحن نصير صُماًّ؟»، كتبته قبل بضعة أشهر لجنة مجلس الشيوخ المختارة المعنية بالاستخبارات. خَلُص التقرير إلى أن وكالة الأمن القومي، التي كانت يوما في طليعة تكنولوجيا استخبارات الإشارة، قد فشلت في مُواكبة ما يحدث من تغيرات في الاتصالات الدولية الشاملة وبينما كان العالم يتحول إلى الهواتف الجوالة الرقمية، والبريد الإلكتروني المُشَّفَر، والألياف الضوئية، بقيت فورت ميد متشبثة جدا وأكثر من اللازم بالتنصُّت على خطوط الهاتف الأرضي، والدوائر التماثلية، واعتراض بث الترددات الراديوية.

كتب التقرير المجموعة الاستشارية التقنية[6]، وهي جماعة صغيرة من الخبراء كانت لجنة مجلس الشيوخ قد جمعتها في العام 1997 لتحليل تداعيات العصر الرقمي الذي يلوح في الأفق. كان معظم أعضاء المجموعة هم من مسؤولي وكالة

الأمن القومي المتقاعدين، الذين كانوا قد حشوا معارفهم في لجنة مجلس الشيوخ على تكوين المجموعة الاستشارية، تحديدا لأنهم كانوا قلقين بشأن وسائل «فورت ميد» العنيدة الجامحة، وظنوا أن استنهاضا خارجيا، لاسيما من أعضاء مجلس الشيوخ الذين يتحكمون في مواردها المالية، ربما يدفع الأمور إلى الأمام قدما.

أحد أعضاء المجموعة، والمعد الرئيسي لهذا التقرير (على الرغم من عدم ذكر اسمه)، كان هو بيل ستوديمان، المدير السابق لوكالة الأمن القومي. كان قد مضى عقدٌ كامل منذ أن أوصى ستوديمان بإجراء دراستين رئيسيتين عند وصوله إلى «فورت ميد»؛ كانت الدراسة الأولى تتوقع وتبين مدى السرعة التي كان العالم سيتحول بها من التماثلية إلى الرقمية. في حين خلصت الدراسة الأخرى إلى أن مجموعات مهارات موظفي وكالة الأمن القومي كانت غير ملائمة لمتطلبات العالم الجديد المرتقب.

في الأعوام التي أعقبت ذلك، كان ستوديمان قد شغل منصب نائب مدير وكالة الاستخبارات المركزية، وانضم إلى كثير من المجالس الاستشارية الاستخباراتية، وترأس مشروعات بشأن الاستطلاع ووسائل حرب المعلومات؛ بوصفه نائب رئيس «مؤسسة نورثروب غرومان» Northrop Grumman Corporation. باختصار، كان ستوديمان لايزال عاملا، وروَّعه الحد الذي وصل إليه تقادم وكالة الأمن القومي.

أخذت لجنة مجلس الشيوخ تقريره بجدية بالغة[7]، مستشهدة به في تقريرها السنوي، ومهددة بخفض موازنة وكالة الأمن القومي إذا لم تُحدِّث ممارساتها لتكون مواكبة للعصر.

جرى تعميم تقرير «ستوديمان» حينما كان مينيهان لايزال مديرا لوكالة الأمن القومي، وأغضبه التقرير. كان مينيهان بالفعل قد حض على كثير من الإصلاحات، وكانت الوكالة قد قطعت شوطا طويلا، منذ أن اكتشفت لجنة مجلس الشيوخ أنها كانت لا تنفق سوى مليوني دولار سنويا على مشروعات النفاذ في الإنترنت، لكنه لم يجاهر بأنه ضد التقرير. إذا صدق أعضاء مجلس الشيوخ التقرير، فهم ربما كانوا سيعززون موازنة وكالة الأمن القومي. تلك كانت مشكلته الكبرى، كان مينيهان يعرف ما ينبغي القيام به، ولم يكن يحتاج سوى مزيد من المال لتنفيذه.

لكن حينما جاء هايدن وتولى «فورت ميد» أخذ تقرير ستودمان على أنه حقيقة لا ريب فيها، وعين مجموعة من خمسة أشخاص خارجيين، من كبار المديرين التنفيذيين لدى مقاولي (متعهدي) الطيران الذين كانوا قد تولوا إدارة عدة مشروعات ذات صلة بالاستخبارات؛ لتجري المجموعة فحصا ومراجعة لهيكلة وكالة الأمن القومي، وثقافتها، وإدارتها، وأولوياتها. وبتشجيع من هايدن، عكفت المجموعة على دراسة السجلات، وأجرت مقابلات مع أكثر من مائة مسؤول، بعضهم من داخل وكالة الأمن القومي، وبعضهم من دوائر أخرى كانت لديها تعاملات مع «فورت ميد»، وفي بعض الحالات كانت هناك تعاملات خفية شائكة مثيرة للجدل.

في 12 أكتوبر، بعد شهرين من التقصي، أطلع أعضاء المجموعة هايدن على النتائج التي توصلوا إليها، ولخصوها بعد ذلك في تقرير يتألف من سبع وعشرين صفحة، كتبوا فيه أن وكالة الأمن القومي كانت تعاني «رداءة في تعريف مهمتها»[8]، و«غياب الرؤية»، و«نظام عاملين معطوبا»، وعلاقات «واهنة سيئة» مع الدوائر الأخرى التي كانت تعتمد على معلوماتها الاستخباراتية، و«ثقافة انغلاقية متقوقعة»، تنبع جزئيا من تكتمها الشديد. نتيجة لكل هذه النقائص، كان مديرو وكالة الأمن القومي يميلون إلى حماية «البنية الأساسية القديمة الموروثة» بدلا من تطوير «أساليب جديدة للتعامل مع الشبكة العالمية الشاملة». إذا أصرت الوكالة على المضي بأساليبها العتيقة البالية التي عفى عليها الزمن، فإنها «ستفشل»، وأن «المستفيدين» - الرئيس، ووزير الدفاع، وغيرهما من كبار المسؤولين - «سيلجأون إلى جهة أخرى» للحصول على ما يحتاجون إليه من معلومات استخباراتية.

كان جزء من بضع ملاحظات أو انتقادات المجموعة جديدا. على مدار عشرين عاما، كان مديرو وكالة الأمن القومي قد تحدثوا بشأن ما كان يلوح في الأفق من فجوة بين أدوات الوكالة والعالم الرقمي القادم. كان ستودمان ومرشده بوبي راي إنمان، يحذران من الحاجة إلى التكيف والمواءمة، على الرغم من أن ذلك كان سابقا لعصره كثيرا لتكتسب كلماتهم زخما. استحث مايك ماكونيل الماكينة على الحركة، لكنه بعد ذلك علق في «رقاقة كليبر» المشؤومة. مقارنة بالأغلبية، كان كين مينيهان يرى المستقبل بوضوح، لكنه لم يكن مديرا بطبيعته. كان مينيهان رجلا طيبا من

تكساس، وفي غنى عن رسميات معظم كبار الضباط، وكان يبالغ في طراز دياره، كان البعض يطلقون على هذا النمط أنه مسحة أندي غريفيث Andy Griffith(*). كان محبوبا من الجميع، لكن لم يكن أحد يفهم ما كان يتحدث بشأنه سوى عدد قليل. كان مينيهان يطرح أقوالا مأثورة (الفلسفة القديمة) في سلاح الجو، مثل «نحن سنقوم بانعطاف حاد جدا ونحن من دون غمامات»(**)، التي كانت تحلق بعيدا فوق فهم واستيعاب الجميع. كان مينيهان قد أطلق شعارات بليغة، مثل «فريق واحد، مهمة واحدة»، ولكن هذا أيضا ما كان يوحي إلا بعدم اليقين والغموض، إذ إنه بدا كأنه يقول إن شخصا ما كان ينبغي أن يعمل بشكل وثيق مع شخص آخر، لكن من، ومع من، استخبارات الإشارة (سيجينت) ومديرية ضمان المعلومات؟ وكالة الأمن القومي ووكالة الاستخبارات المركزية؟ أجهزة الاستخبارات والجيش؟ لم يكن أحد يعرف على وجه التحديد.

على النقيض، كان هايدن جنرالا عسكريا عصريا، أقل اندفاعا، وبالطبع لم يكن شعبيا متواضعا مثلما كان مينيهان، وكان بدرجة أكبر مديرا شديد البأس في مواجهة المواقف الصعبة، ويجيد وضع الرسوم التخطيطية. وعلى سبيل المتابعة للإحاطة التي قدمتها مجموعة الرجال الخمسة، كان هايدن قد أعد بنفسه مذكرة من ثماني عشرة صفحة بعنوان «خطة عمل المدير من أجل التغيير» التي صاغها في كلمات صريحة بلا مواربة، ملخصا كثيرا من تقرير المديرين التنفيذيين، وموجزا الخطوط العريضة للحلول المقترحة في التقرير. وقد عمم المذكرة في كل أرجاء وكالة الأمن القومي.

كانت صياغة هايدن اللغوية حادة وصارمة مثلما كانت رسالته. كتب هايدن أن وكالة الأمن القومي «منظمة غير متسقة»[9]، وتراثها السابق العريق «في خطر كبير». كانت وكالة الأمن القومي في حاجة إلى قيادة جديدة جريئة، وقوة عاملة متكاملة يتناغم فيها عمل استخبارات الإشارات مع عمل أمن المعلومات، على ألا يكون أي منهما على خلاف مع الآخر (هذا ما كان مينيهان قد قصده من مقولة

(*) أندي غريفيث Andy Griffith (1926/2012) كان ممثلا أمريكيا كوميديا، ومنتجا للتلفزيون، وكاتبا، امتد عمله طوال سبعة عقود في مجال الموسيقى والتلفزيون، اشتهر بتشدقه في الكلام بلكنة الجنوب الأمريكي، وشخصيته الشعبية الودودة، وصوته الأجش. [المترجم].

(**) المقصود توسيع الأفق. [المترجم].

«فريق واحد، مهمة واحدة»)، وقبل كل شيء مديرية استخبارات الإشارة التي يعاد توجيه تركيزها، والتي كانت سوف «تتصدى لتحدي التغير التكنولوجي».

واختتم هايدن: «إننا فهمنا الأمر على نحو عكسي. نحن نبدأ بمهاراتنا الداخلية؛ إيمانا منا بأن الفائدة ستعود على زبائننا في نهاية المطاف»، في حين أنه في واقع الأمر، كانت الوكالة تحتاج إلى التركيز أولا على احتياجات الزبائن (البيت الأبيض، ووزارة الدفاع، وبقية أجهزة الاستخبارات)، ثم مواءمة مهاراتها الداخلية وفقا لتلك المهام.

كان مينيهان قد قطع شوطا في هذا الطريق، وحطم المجموعة «أ»، المختصين في الشؤون السوفييتية الذين كانوا قد ساعدوا على كسب الحرب الباردة، لكنه لم يقم هيكلا، ولم يعرف مهمة جديدة جلية المعالم تستحق لقب المجموعة «أ» لتحل محلها. لم يكن هذا خطأه بالكامل، ومثلما كان كثيرا ما يشكو ويتذمر، كان مينيهان ينقصه المال، والوقت، وأي توجيهات من قيادته السياسية. من الناحية المثالية، مثلما كان هايدن سيلاحظ، كانت وكالة الأمن القومي تذهب وتحصل على ما يريد قادة البلاد أن تحصل الوكالة عليه، ولم يكن أي أحد من أصحاب المناصب العليا يصدر إلى مينيهان أي أمر بالتحرك. ثم مجددا، صار الافتقار إلى التواصل في اتجاهين، لم يكن أحد من أصحاب المناصب العليا يعرف ما الذي كانت وكالة الأمن القومي تستطيع تقديمه غير بضاعتها المعتادة، التي كانت على ما يرام بقدر الإمكان، ولكن دون المستوى في عالم تصير فيه أدوات وتقنيات الوكالة «صماء».

وفقا لتقرير المديرين التنفيذيين في مجال الطيران، كان «نظام العاملين المعطوب» هو إحدى المشكلات الرئيسية للوكالة. كان العاملون بالوكالة في الأغلب يستمرون في الخدمة مدى الحياة، وكانت ترقياتهم في الرتب تتم بوتيرة واحدة ثابتة، وعلى نحو تلقائي تقريبا، مع إيلاء قدر ضئيل من الاعتبار للمهارات الفردية. هذا النظام التنصيبي الجامد القائم على التثبيت، كان قد عرقل محاولات الإصلاح السابقة، فقد احتل المناصب العليا أناس جاءوا في السبعينيات والثمانينيات من القرن العشرين، حينما كانت الأموال تتدفق من دون قيد، وكان العدو محددا واضح المعالم، والاتصالات - بصفة رئيسية المحادثات الهاتفية وعمليات بث التردد الراديوي - كان يمكن التنصت عليها بواسطة دائرة بسيطة، أو بجمعها من الهواء.

بادئ ذي بدء، وقبل كل شيء، غيّر هايدن نظام شؤون الأفراد. في 15 نوفمبر دشن[10] «مائة يوم من التغيير». في السابق، كان كبار الموظفين يرتدون شارات خاصة ويستخدمون مصاعد خاصة. ومن ذلك الحين، كان الجميع سيرتدي شارات واحدة، وكانت كل المصاعد ستفتح للجميع. أيضا عمد هايدن إلى تنقية نظم تقييم العاملين، مستأنسا برأي بضعة مستشارين ثقات. وبعد مرور أول أسبوعين، فصل هايدن من الخدمة ستين شخصا كانوا قد استحوذوا على المكان على مدار عقود، ورقّى ستين مسؤولا أكثر كفاءة لشغل الوظائف الشاغرة، وكان معظمهم أحدث كثيرا في العمر والأقدمية الوظيفية.

أعقب ذلك كثير من التذمر، ولكن في 24 يناير 2000، بعد عشرة أسابيع من بدء حملة هايدن، دق ناقوس خطر، فقد تعطل نظام الحاسب الرئيسي في وكالة الأمن القومي[11]، وبقى كذلك اثنتين وسبعين ساعة. كان الحاسوب لاتزال مخزنة عليه معلومات استخباراتية كانت المحطات الميدانية تجمعها من كل أنحاء العالم، لكن لم يكن أحد في «فورت ميد» يستطيع الوصول إليها. كانت هناك معلومات استخباراتية أولية مجردة عديمة النفع - لم تجرِ غربلتها، وغير معالجة، ولم يجرِ تحليلها. طوال ثلاثة أيام، كان واقع الأمر يقول إن وكالة الأمن القومي معطلة.

في البداية، كان البعض يشتبه في أنها عملية تخريب، أو أنها أثر متأخر ناجم عن مشكلة العام 2000؛ لكن الطاقم التقني بالوكالة استنتج سريعا أن الحاسوب كان قد جرى تحميله على نحو زائد. كان الضرر شديدا جدا، لدرجة أنهم اضطروا إلى إعادة بناء البيانات والبرامج بعد عودة النظام إلى العمل.

توقف التذمر بشأن هايدن. إذا كان أي شخص قد ارتاب في أن التغييرات الضخمة كانت ضرورية، فإنه لم يعد هناك الآن أي شك.

كان تقرير المديرين قد أبرز انتقادا آخر هو أن مديرية استخبارات الإشارة كانت تصنّف قنواتها الناقلة للبيانات تصنيفا جغرافيا. كانت إحدى المجموعات تبحث في الإشارات الصادرة عن الاتحاد السوفييتي السابق، ومجموعة أخرى تبحث في الإشارات الصادرة عن الشرق الأوسط، وثالثة للإشارات الصادرة عن آسيا. في حين أن كل الاتصالات في العالم الحقيقي كانت تمر من خلال شبكة واحدة، الشبكة العنكبوتية العالمية (الويب) The World Wide Web التي كانت - بكل دقة - هي بالفعل عالمية النطاق.

اقترح المديرون التنفيذيون، في تقريرهم، هيكلا تنظيميا جديدا لمديرية استخبارات الإشارة، لم يكن تقسيم بنائه وفقا للخطوط الإقليمية (التي لم تعد منطقية)، لكن بدلا من ذلك كانت أقسامه هي «الاستجابة العالمية الشاملة» Global Response، و«الشبكة العالمية الشاملة» Global Network، و«الولوج المصمم وفقا للحاجة» Tailored Access.

كانت «الاستجابة العالمية الشاملة» ستتعامل مع الأزمات اليومية من دون تحويل موارد وإمكانات الوكالة عن مهامها المستمرة. لقد كان هذا مصدرا كبيرا لإحباطات مينيهان، فقد كان الرئيس، أو وزير الدفاع، يداومان على طلب كم هائل من المعلومات الاستخباراتية بشأن أزمة تلو الأخرى، مثل: تكديس صدام حسين الأسلحة، وبرنامج كوريا الشمالية النووي، وآفاق وتوقعات مباحثات السلام في الشرق الأوسط، إلى حد أنه لم يكن بوسع مينيهان التركيز على الإصلاحات الهيكلية.

كانت «الشبكة العالمية الشاملة» هي التحدي الجديد. في الأيام السابقة كان خبراء اللغة في وكالة الأمن القومي يجلسون ويستمعون إلى البث الحي أو الأشرطة المسجلة، لمحادثات هاتفية والبث الراديوي (اللاسلكي) التي كانت وسائل التنصت وأطباق الاستقبال تتفحصها وتحصدها في جميع أنحاء العالم. في العصر الجديد، عصر الهواتف الجوالة، وأجهزة الفاكس، والإنترنت، فإنه عادة لم يكن هناك أي شيء للاستماع إليه، إلى حد أن الإشارة لم تكن تنتقل من نقطة إلى أخرى عبر خط واحد أو قناة واحدة؛ بدلا من ذلك، تندفع الاتصالات الرقمية عبر الشبكة في حزم بيانات تمتزج بإحكام على نحو وثيق مع حزم لاتصالات أخرى (الخاصية التي كانت أشعلت جدلا كبيرا بعد أعوام لاحقة، حينما علم المواطنون أن وكالة الأمن القومي كانت تعترض محادثاتهم، إلى جانب محادثات الأشرار المجرمين). كانت تلك الشبكات والحزم أكثر اتساعا من أن يرصدها البشر في الوقت الحقيقي. كان ينبغي تقطيع المعلومات الاستخباراتية، وتنقيتها، ومعالجتها بواسطة حواسيب ذات سرعة عالية جدا، وفحص البيانات بحثا عن كلمات دليلية رئيسية، أو أنماط مشبوهة لحركة البيانات.

بالنسبة إلى هايدن، كان تعطل الحاسوب (الذي دام ثلاثة أيام في شهر يناير) يشير إلى أن معدات وكالة الأمن القومي ربما لا ترقى إلى مستوى المهمة. كان المسؤولون التنفيذيون في مجال الطيران، ومن دون أدنى مصلحة شخصية، قد أوصوا بضرورة

فحص الوكالة ما يمكن أن يقدمه المقاولون (المتعاقدون) الخارجيون. أخذ هايدن بمقترحهم. كان الأمر سيتطلب حواسيب وبرمجيات جديدة لفحص واستيعاب هذه الشبكة العالمية الشاملة الجديدة، وربما كان المقاولون الخارجيون سيتمكنون من العمل على نحو أفضل لإيجاد واستحداث مثل هذه الحواسيب والبرمجيات.

أطلق هايدن على البرنامج الجديد اسم «الرائد» Trailblazer[12]، وفي أغسطس عقد «يوم الرائد للصناعة» Trailblazer Industry Day، داعيا 130 من ممثلي الشركات إلى المجيء إلى «فورت ميد» والاستماع إلى مخططه. في أكتوبر افتتح منافسة على تعاقد لبناء «منصة إيضاحية للعرض التقني»(*) للنظام الجديد. في مارس اللاحق منحت وكالة الأمن القومي مبلغ 280 مليون دولار - وهو مخصص افتتاحي لما كان سيزيد على مليار دولار على مدى السنوات العشر اللاحقة لـ «المؤسسة الدولية للتطبيقات العلمية) Science Applications International Corporation، مع أجزاء من البرنامج، مشاركة بين شركة «نورثروب غرامان» Northrop Grumman، و«بوينغ» Boeing، و«مؤسسة كومبيوتر ساينس» Computer Sciences Gorp، و«بووز آلين هاميلتون» Booz Allen Hamilton، وجميعها كانت لها - منذ فترة طويلة - علاقات مع الأوساط الاستخباراتية.

كانت «المؤسسة الدولية للتطبيقات العلمية»، بوجه خاص، متداخلة جدا[13] مع وكالة الأمن القومي، وكان بوبي راي إنمان عضوا في مجلس إدارتها. كان بيل بلاك Bill Black، أحد كبار خبراء التشفير في الوكالة، قد تقاعد في العام 1997 ليصير نائبا مساعدا لرئيس المؤسسة، ثم بعد مضي ثلاثة أعوام، في واقعة من تطبيق سياسة «الأبواب الدوارة» Revolving Doors صدمت وأذهلت المنتمين إلى الوكالة حتى أكثرهم فجرا؛ إذ إن بلاك أعاده هايدن ثانية ليكون نائبا لمدير وكالة الأمن القومي، وليتولى إدارة برنامج «الرائد» Trailblazer، كان يتولى إداراته من الجانب الآخر من الجسر في « المؤسسة الدولية للتطبيقات العلمية».

مع ذلك، كانت وكالة الأمن القومي لاتزال في حاجة إلى انطلاقة أكبر، كانت تحتاج إلى أدوات وتقنيات لاعتراض الإشارات، ليس فقط في أثناء تدفقها عبر الشبكة

(*) «منصة إيضاحية للعرض التقني» هي نموذج أولي، أو مثال تقريبي، أو نسخة غير مكتملة من منتج أو نظام مستقبلي، بهدف أساسي هو عرض التطبيقات الممكنة، وإمكان وجدوى، وطريقة فكرة تقنية جديدة. [المترجم].

الرقمية، لكن أيضا عند مصادرها. كان ما حدث في «البلقان» من اختراق لنظام الهاتف في بلغراد هو أكبر حملة لوسائل حرب المعلومات حتى ذلك الوقت. في أوائل ذاك العقد، في حرب الخليج، حينما كان جنرالات صدام حسين يرسلون أوامرهم عبر كابل الألياف الضوئية، فإن لجنة الاستخبارات المشتركة بالبنتاغون، التي كانت على نحو كبير تعتمد على أفراد وتقنيات وكالة الأمن القومي، اكتشفت الكيفية التي من خلالها تنسف روابط الكابل، مما أجبر صدام على التحول إلى الموجات الميكروويية. كانت وكالة الأمن القومي تعرف كيفية اعتراض الموجات الميكروويية، لكنها لم تكن تعرف بعد كيفية اعتراض البيانات التي تندفع عبر الألياف الضوئية، وهذا هو ما كانت الوكالة تحتاج إلى فعله حينذاك.

أوصى التنفيذيون في مجال الطيران، في تقريرهم إلى هايدن، بأن تعمل مديرية استخبارات الإشارة على نحو وثيق مع مديرية ضمان المعلومات؛ لأن مهماتها كانت «تصبح سريعا وجهين لعملة واحدة».

طوال عدة أعوام، فإن مديرية ضمان المعلومات، التي مقرها في ملحق بالقرب من مطار بالتيمور - واشنطن الدولي، على بعد نصف ساعة بالسيارة من «فورت ميد»، كانت تختبر وتصلح البرمجيات التي كان جيش الولايات المتحدة يستخدمها، وذلك بحثا عن أوجه ضعف أو ثغرات أمنية يمكن أن يستغلها العدو. حاليا، أحد الأدوار الرئيسية لأطقم استخبارات الإشارة، في قلب المقر الرئيسي للوكالة، كان هو اكتشاف أوجه الضعف والثغرات الأمنية في برمجيات الخصوم واستغلالها. ولأن آحاد الناس (والمؤسسات العسكرية) في جميع أنحاء العالم كانوا يستخدمون البرمجيات الغربية نفسها، كان اختصاصيو مديرية ضمان المعلومات يمتلكون المعرفة التي كانت ستعود بالنفع على أطقم استخبارات الإشارة في الوقت ذاته، كان لدى فرق استخبارات الإشارة دراية بشبكات الخصوم؛ ماذا كانوا يفعلون، وما أنواع الهجمات التي كانوا يخططون لها ويختبرونها؟ مما كان سيعود بالنفع على اختصاصيي مديرية ضمان المعلومات. كان تشارك هذه المعرفة، بشأن الهجوم والدفاع، يتطلب مزج هاتين الثقافتين المنفصلتين.

كان إنمان وماكونيل قد اتخذا خطوات نحو هذا التكامل. كان مينيهان قد بدأ في إزالة الحواجز، ونقل بضعة أفراد من الملحق إلى المقر الرئيسي والعكس بالعكس.

كان هايدن يتوسع فيما قام به مينيهان من توزيع، بتحريك مزيد من الأفراد جيئة وذهابا بين الجهتين، لاكتساب فهم أعمق بشأن أمن عملياتهم.

كانت هناك قضية أخرى لا بد من فض تشابكها، وهي تقسيم العمل داخل أجهزة الاستخبارات، لاسيما بين وكالة الأمن القومي ووكالة الاستخبارات المركزية. في الأيام السابقة، كان هذا التقسيم واضحا؛ إذا تحركت المعلومات، كانت وكالة الأمن القومي ستعترضها؛ أما إذا بقيت ساكنة بلا حركة، فإن وكالة الاستخبارات المركزية كانت سترسل جاسوسا للعثور عليها وأخذها. كانت وكالة الأمن القومي تعترض الإلكترونات التي تقرقع في الهواء أو عبر خطوط الهاتف، وكانت وكالة الاستخبارات المركزية تسرق وثائق قابعة فوق مكتب أو داخل قبو. لقد كان الخط الفاصل مرسوما بوضوح طوال عدة عقود. لكن في العصر الرقمي صار الخط الفاصل ضبابيا مشوشا. أين تقع الحواسيب من هذا الخط الفاصل؟ إنها تخزن البيانات على الأقراص المرنة والأقراص الصلبة، التي هي ساكنة غير متحركة، لكنها أيضا كانت ترسل البتّات والبايتات bits and bytes عبر الفضاء السيبراني. في كلتا الحالتين كانت المعلومات هي ذاتها، ومن ثم من الذي كان ينبغي أن يحصل عليها: «لانجلي» أم «فورت ميد»؟

كانت الإجابة المنطقية هي، كلاهما. لكن إنجاز مثل هذا العمل الفذ كان سيحتاج إلى اندماج، مع قليل من التمهيد القانوني أو الإداري. على مر الأعوام، كان هناك تعاون بين وكالتي التجسس في مشروعات عرضية عابرة، ولكن هذه الحال الجديدة كانت ستنطوي على خلط مؤسسي للمهام والوظائف؛ ولكي تقوم كل وكالة بدورها، كان سيتعين على كل منهما استحداث كيان جديد، أو أن تعمل على إعادة هيكلة وإعادة توجيه أحد الكيانات القائمة.

واقع الأمر أنه تصادف أن إطارا لهذا الاندماج كان موجودا بالفعل. في أثناء عملية بلغراد كانت وكالة الاستخبارات المركزية قد استحدثت «مركز عمليات المعلومات» Information Operations Center، بغرض غرس أجهزة في أنظمة الاتصالات الصربية، لكي تستطيع وكالة الأمن القومي اعتراضها بعد ذلك. كان هذا المركز سيصير هو مساهمة لانجلي في الجهود المشتركة الجديدة، أما «فورت ميد» فكانت ستسهم بالصندوق الثالث من الهيكل التنظيمي الجديد لمديرية استخبارات الإشارة - «الولوج المصمم وفقا للحاجة».

كان مينيهان هو الذي قد نحت العبارة. في أثناء فترة ولايته مديرا، كان ينتقي بضع عشرات من أكثر رجال عمليات استخبارات الإشارة إبداعا، وكان يجمعهم في ركن خاص بهم في الطابق الرئيسي، ويسند إليهم تلك المهمة. ما قد كان يضطلع عناصر عمليات الحقائب السوداء السرية في وكالة الاستخبارات المركزية في العالم المادي فترة طويلة، حاليا كان طاقم «الولوج المصمم وفقا للحاجة» سيضطلع به في الفضاء السيبراني، وفي بعض الأحيان جنبا إلى جنب مع عناصر عمليات الحقائب السوداء السرية، إذا استلزم الأمر تنصيب أحد الأجهزة أو الأدوات على إحدى المعدات الحيوية بالغة الأهمية، مثلما حدث في بلغراد.

حوّل هذا الترتيب مفهوم استخبارات الإشارات، وهي رصيد وكالة الأمن القومي الذي كان يميزها. لقد كانت استخبارات الإشارة فترةً طويلة تُعرف على أنها التقاط جميع الإلكترونات الشاردة في الأثير وجمعها على نحو سلبي بلا تدخل فاعل. حاليا، كان الأمر سينطوي أيضا على الاختراق الفاعل والولوج إلى الأجهزة والشبكات الرقمية.

كان مينيهان قد رغب في توسيع مهمات «الولوج المصمم وفقا للحاجة» لتصير هي المجموعة «أ» للعصر الرقمي، لكنه استنفد كل الوقت. حينما ابتدأ هايدن إعادة الهيكلة، أخذ بزمام الأمور وحوّلها إلى هيئة متميزة مستقلة ونخبوية، ألا وهي «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو) Office of Tailored Access Operations (TAO).

حتى في إطار ما كان يضطلع به هايدن من توسيع لنطاق مهماته، بدأ «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو) باعتباره طاقما صغيرا، بضع عشرات من مبرمجي الحاسوب، الذين كان ينبغي لهم اجتياز اختبار عسير جدا حتى يمكنهم الانضمام إليه. سرعان ما نمت المنظمة لتصير فريقا من النخبة، محاطا بالسرية والكتمان، ومحجوبا عن بقية وكالة الأمن القومي، مثلما كانت وكالة الأمن القومي بالنسبة إلى بقية مؤسسة الدفاع. كان مقره في جناح منفصل في «فورت ميد»، وكان مادة للتهامس بإشاعات خلت من معرفة حقيقية، حتى بين أولئك الذين - عدا ذلك - كانت لديهم صلاحيات أمنية رفيعة المستوى. كان أي شخص يسعى إلى الدخول إلى عرينها، يجب عليه المرور بحارس مسلح، وباب موصد بأقفال مشفرة، وماسح ضوئي لبصمة شبكية العين.

في الأعوام التالية، كانت صفوف «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو) ستزداد وتتضخم[14] لتصل إلى ستمائة من «رجال عمليات الاعتراض» في «فورت ميد»، بالإضافة إلى أربعمائة أو أكثر في منافذ وكالة الأمن القومي – التي كان يطلق عليها مراكز العمليات القاصية – في واهياوا Wahiawa بولاية هاواي Hawaii، وفورت جوردون Fort Gordon بولاية جورجيا Georgia، وقاعدة «باكلي» الجوية بالقرب من مدينة دينفر Denver، ومركز تكساس لعلم الشفرة في مدينة سان أنطونيو San Antonio.

كانت مهمة «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو)، وشعارها غير الرسمي، هما «الحصول على ما لا يمكن الحصول عليه»، وتحديدا الحصول على ما كان لا يمكن الحصول عليه مما كانت تريده القيادة السياسية للوكالة. إذا رغب الرئيس في معرفة ما الذي يفكر فيه ويفعله زعيم إرهابي، فإن «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو) كان سيتعقب حاسوب ذلك الزعيم الإرهابي، ويخترق محرك الأقراص الصلبة خاصته، ويسترجع ملفاته، ويعترض بريده الإلكتروني، في بعض الأحيان من خلال الفضاء السيبراني فقط (لا سيما في الأيام الأول، حينما كان من السهل كسر كلمة المرور الخاصة بالهدف، إذا كان قد أدرج كلمة مرور أساسا)، وفي أحيان أخرى بمساعدة جواسيس من وكالة الاستخبارات الأمريكية أو جنود الظل الموازين من رجال العمليات الخاصة، الذين يكونون قد وضعوا أيديهم على الحاسوب وأدخلوا به ناقلة بيانات (وحدة ذاكرة فلاشية) محملة ببرامج ضارة، أو وضعوا أحد الأجهزة (الأدوات) التي كان أحد متخصصي «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو) سيولج إلى الحاسوب من خلاله.

كانت طرائق تشغيل ووجود تلك الأجهزة[15] مصنفة على أنها سرية جدا، حتى إن تصميم وبناء معظمها كانا يتمان داخل وكالة الأمن القومي، البرمجيات بواسطة «فرع تكنولوجيات شبكة البيانات»، والتقنيات بواسطة «فرع تكنولوجيات شبكة الاتصالات»، وطرفيات الحاسوب والشاشات المعدلة وفقا للطلب بواسطة «فرع تكنولوجيات البنية الأساسية».

في المراحل الأولى، كان «مكتب عمليات الولوج المصمم وفقا للحاجة» يخترق الحواسيب بطرق بسيطة جدا، مثل: التصيد الاحتيالي (الانتحال) لكلمات المرور

(مثل هذه البرامج تجرب كل كلمة في القاموس، بالإضافة إلى تنويعات وأرقام، في جزء من الثانية)، أو إرسال رسائل بريد إلكتروني مصحوبة بمرفقات مغرية تستطيع تنزيل برمجيات ضارة حينما تُفتح. ذات مرة وُجهت دعوة إلى بعض محللي «فريق العمل المشترك لعمليات شبكات الحاسوب» (جيه تي إف-سي إن أوو) لزيارة «فورت ميد» لإلقاء نظرة على الحيل التي لدى «مكتب عمليات الولوج المصمم وفقا للحاجة». ضحك المحللون، إنها لم تكن تختلف كثيرا عن البرمجيات التي كانوا قد شاهدوها أخيرا في مؤتمر «ديف كون» DEF Con للقرصنة(*)، بعض البرمجيات كانت تبدو كأنها إصدار أُعيد تجميعه من البرمجية نفسها.

على الرغم من ذلك، كانت فرق «مكتب عمليات الولوج المصمم وفقا للحاجة» تعمل على صقل مهاراتها وتنمية ترسانتها تدريجيا. اكتشفوا نقاط دخول خفية في المخدمات، والموجهات **routers**، ومحطات العمل **workstations**، وسماعات الهاتف، ومبدلات الهاتف، وحتى في جدران حماية (الجدران النارية) **firewalls** (التي، من دواعي السخرية، كان من المفترض أنها لإبعاد المتسللين)، وكذلك في برمجيات إدارة تلك المعدات، والشبكات التي تربطها. ومع تطور مجال عملهم، أصبحت أجهزتهم وبرامجهم تشبه شيئا خرج من أكثر أفلام جيمس بوندJames Bond غرابة. أحد الأجهزة، يسمى «لاود أوتو» **LoudAuto**[16]، كان ينشط ميكروفون الحاسوب النقال، ويرصد أحاديث أي شخص في الجوار؛ هاولر مانكي **HowlerMonkey**، كان يستخلص الملفات ويرسلها عبر الإشارات الراديوية (اللاسلكية)، حتى إن كان الحاسوب غير موصول بالإنترنت؛ مانكي كالندر **MonkeyCalendar**، كان يتتبع موقع هاتف جوال وينقل المعلومات من خلال «رسالة نصية» **NightStand**، كان نظاما لاسلكيا نقالا، يحمّل برامج ضارة على جهاز حاسوب على بعد أميال عدة؛ ريج ماستر **RageMaster**، كان يتنصت على إشارة الفيديو الخاصة بالحاسوب، بذلك كان أحد فنيي «مكتب عمليات الولوج المصمم وفقا للحاجة» سيتمكن من رؤية ما الذي كان على شاشة الحاسوب المخترق، ومن ثم يشاهد ما كان يشاهده الشخص المستهدف.

(*) ديف كون DEF Con هو أحد أكبر المؤتمرات العالمية لقراصنة الحاسوب، يعقد سنويا في لاس فيغاس، نيفادا. [المترجم].

لكن مع نضج «مكتب عمليات الولوج المصمم وفقا للحاجة»، وكذلك نضج من كان يستهدفهم، اكتشف أساليب لكشف المتسللين وصدهم، تماما مثلما كان البنتاغون وسلاح الجو قد توصلا في العقد الماضي إلى طرائق لاكتشاف وصد اختراقات الخصوم، ومجرمي السيبرانية، والمشاغبين النازعين للأذى. كلما كان قراصنة الحاسوب والجواسيس يكتشفون أوجه ضعف وثغرات أمنية[17] في برمجيات وأجهزة الحاسوب، كان المصنعون يعملون جاهدين لسد الثغرات، الأمر الذي كان يحفّز قراصنة الحاسوب والجواسيس على البحث عن أوجه ضعف وثغرات أمنية جديدة، وهكذا كان السباق يتصاعد.

بينما كان هذا السباق بين القرصنة والترميم لتصحيح الثغرات الأمنية وسدها آخذا في التصاعد، بدأ الممارسون لكلا نوعي الفنون، في جميع أنحاء العالم، بإيلاء أهمية كبيرة لـ «الثغرات الأمنية التي يمكن استغلالها على نحو فوري دون انتظار» «نقاط الضعف الفورية» zero-day vulnerabilities، تلك الفجوات التي لم يكن أحد قد اكتشفها بعد، فضلا عن رتقها وإصلاحها. في العقد اللاحق، كانت ستنطلق شركات خاصة[18] جنت في بعض الحالات ثروات صغيرة من العثور على «نقاط الضعف الفورية» وبيع اكتشافاتها لحكومات، وجواسيس، ومجرمين، لهم دوافع متباينة، ومن جنسيات مختلفة. كان هذا القنص لـ «نقاط الضعف الفورية» يشغل بعضا من العقول الأكثر حنكة في الرياضيات، في وكالة الأمن القومي وغيرها من الجماعات السيبرانية، في الولايات المتحدة وخارجها.

ذات مرة، في أواخر التسعينيات من القرن العشرين، اكتشف ريتشارد بيجليك Richard Bejtlich، وهو محلل دفاع شبكة الحاسوب في قاعدة كيلي الجوية، اكتشف إحدى «نقاط الضعف الفورية» في إحدى الموجهات router الذي تنتجه شركة سيسكو Cisco، وكان ذلك اكتشافا نادرا. اتصل بيجليك هاتفيا بأحد التقنيين في شركة سيسكو، وأبلغه بالمشكلة، فأصلحها ممثل الشركة على وجه السرعة.

بعد بضعة أيام، فخورا ببراعته وصنيعه الحسن، روى بيجليك القصة لمحلل كان يعمل في قاعدة كيلي الجوية في الجانب الهجومي. لم يكن المحلل مسرورا، وقال متمتما، وهو متحفز ويحدق بحدة في بيجليك: «لماذا لم تخبرنا؟».

كان التلميح واضحا، إذا كان بيجليك قد أخبر المحللين في الجانب الهجومي بشأن ذلك العيب، فربما كان باستطاعتهم استغلاله في اختراق الشبكات الأجنبية التي كانت تستخدم مخدم سيسكو. الآن فات الأوان، بفضل اتصال بيجليك الهاتفي، صُححت الثغرة وعولجت، وأُغلقت البوابة.

بينما كانت وكالة الأمن القومي تولي مزيدا من الاهتمام لاكتشاف واستغلال أوجه الضعف والثغرات الأمنية، برزت فئة جديدة من العمليات السيبرانية. في السابق، كانت هناك «حماية شبكات الحاسوب» (سي إن دي) Computer Network Defense (CND) و«مهاجمة شبكات الحاسوب» (سي إن أيه) Computer Network Attack (CNA)؛ الآن أصبح هناك أيضا «استغلال شبكة الحاسوب» (سي إن إي) Computer Network Exploitation (CNE).

كان «استغلال شبكة الحاسوب» (سي إن إي) مبادرة ملتبسة من الوجهتين القانونية والتشغيلية (العملياتية)، وكان هايدن يعرف ذلك، وهو كان حساسا تجاه الضرورات القانونية ويراعي التفاصيل القانونية الدقيقة ومحدودية ما تسمح به من مرونة ومجال للمناورة. كان المعنى التقني للمصطلح مباشرا وصريحا، وهو استخدام الحاسوب لاستغلال أوجه الضعف والثغرات الأمنية في شبكات الخصم، والاستفادة بها للولوج إلى تلك الشبكات من أجل كسب مزيد من المعلومات الاستخباراتية عنهم. لكن كانت هناك طريقتان للنظر إلى «استغلال شبكة الحاسوب» (سي إن إي). كان يمكن أن تكون خط المجابهة لـ «حماية شبكات الحاسوب» (سي إن دي)، استنادا إلى منطق مُفاده أن أفضل طريقة للدفاع عن الشبكة هي معرفة ما لدى الخصم من خطط للهجوم، الأمر الذي كان يتطلب الولوج إلى شبكته. أو أن ينظر إلى «استغلال شبكة الحاسوب» (سي إن إي) على أنه هو البوابة لـ«هجوم شبكات الحاسوب» (سي إن أيه)، الولوج إلى شبكة العدو من أجل رسم خرائط ممراتها وتحديد نقاط ضعفها من أجل «إعداد ساحة المعركة» (كما كان سيُطلق عليها قادة العصور القديمة) لهجوم أمريكي، في حالة نشوب الحرب(*).

(*) انبثقت من «استغلال شبكة الحاسوب» (سي إن إي) تقسيمات فرعية لاستخبارات الإشارة أكثر ابتكارا، مثل: «سي-سي إن إي C-CNE»، وتعني «مكافحة استغلال شبكات الحاسوب» Counter-Computer Network Exploitation، وهي النفاذ إلى شبكات أحد الخصوم من أجل مراقبته وهو ينفذ إلى شبكاتنا.

كان مفهوم «استغلال شبكة الحاسوب» (سي إن إي) مناسبا تماما لرغبة هايدن في صهر الهجوم السيبراني مع الدفاع السيبراني ليتعذر تمييز أي منهما؛ وبينما كان هايدن قد أعرب عن المفهوم بأسلوب كان يناسب أجندته، فإنه لم يخترعه. بالأحرى، كان المفهوم يعكس جانبا متأصلا في شبكات الحاسوب الحديثة ذاتها.

من ناحية، لم يكن «استغلال شبكة الحاسوب» (سي إن إي) يختلف كثيرا عن جمع المعلومات الاستخباراتية في العصور السابقة. في أثناء الحرب الباردة، كانت طائرات تجسس أمريكية تنفذ عبر الحدود الروسية لإجبار الضباط السوفييت على تشغيل أجهزة الرادار لديهم، ومن ثم تتكشف معلومات بشأن ما لديهم من أنظمة دفاع جوي. كانت طواقم الغواصات تتنصت على الكابلات تحت الماء بالقرب من الموانئ الروسية لاعتراض الاتصالات البحرية السوفييتية، واكتشاف نسق عملياتها. كان لهذا أيضا غرض مزدوج، هو تعزيز الدفاعات ضد أي عدوان سوفييتي محتمل، وإعداد ساحة المعركة (أو المجال الجوي والمحيطات) لهجوم أمريكي.

لكن من ناحية أخرى، فإن «استغلال شبكة الحاسوب» (سي إن إي) كان مبادرة مختلفة كلية، إذ إنه كان يعرض المجتمع بأسره لأخطار ومخاوف المغامرات العسكرية على نحو لم يكن في الإمكان تخيله قبل بضعة عقود. حينما كان المسؤولون في سلاح الجو أو في وكالة الأمن القومي يتجاهلون إبلاغ شركة مايكروسوفت (أو سيسكو أو غوغل أو إنتل أو أي شركات أخرى) بشأن أوجه الضعف والثغرات الأمنية في برمجياتها، وحينما كانوا يتركون فجوة من دون أن تُسد حتى يستطيعوا استغلال الثغرة الأمنية في أنظمة الحاسوب الروسية، أو الصينية، أو الإيرانية، أو التي لدى بعض الخصوم الآخرين؛ فإنهم بذلك كانوا أيضا يدعون المواطنين الأمريكيين معرضين إلى ذات الاستغلال، سواء من دوائر استخبارات أو مجرمين سيبرانيين، أو جواسيس أجانب، أو إرهابيين يتصادف أنهم أيضا عرفوا بشأن الفجوة التي لم تُسد.

كان هذا توترا جديدا في الحياة الأمريكية، ليس فقط بين حرية الفرد والأمن القومي (لقد كان ذلك موجودا دائما بدرجات متفاوتة)، ولكن أيضا بين مختلف طبقات ومفاهيم الأمن. في أثناء إجراءات الحفاظ على الشبكات العسكرية أكثر أمنا في مواجهة الاعتداء، كان المحاربون السيبرانيون يجعلون الشبكات المدنية (غير العسكرية) والتجارية أقل أمانا في مواجهة ذات الأنواع من الاعتداء.

تلك التوترات، وما أثارته من قضايا، تجاوزت حدود دواوين الجهاز الإداري للأمن القومي. لم يكن أحد يستطيع فضها سوى القادة السياسيين. مع اقتراب القرن الحادي والعشرين، كانت إدارة كلينتون قد بدأت استيعاب تعقيدات الموضوع، لاسيما في أثناء الحشد المحموم لمصلحة ديك كلارك Dick Clarke. كان هناك تقرير مارش، متبوعا بـالتوجيه «بي دي دي63-» PDD-63 المتعلق بحماية البنية الأساسية الحرجة، و«الخطة القومية لحماية نظم المعلومات» National Plan for Information Systems Protection، واستحداث مراكز لتشارك وتحليل المعلومات، وهي منتديات كانت الحكومة من خلالها تستطيع العمل مع الشركات الخاصة لاستنباط أساليب لتأمين ما لديها من أصول ضد الهجمات السيبرانية.

ثم جاءت انتخابات نوفمبر من العام 2000، وكما كان يحدث عادة حينما يتغير الحزب في البيت الأبيض، توقف تماما كل هذا الزخم. حينما وصل جورج دبليو بوش (الابن) George W. Bush ومعاونوه إلى السلطة في 20 يناير من العام 2001، تأجج ما كانوا يخفونه من ازدراء واحتقار لأسلافهم مصحوبا بضغينة وغل على نحو أكثر من المعتاد، بسبب الفضيحة الجنسية والطعن في صدق الشهادة التي شوهت الفترة الثانية من ولاية كلينتون، والتي تفاقمت بسبب العواقب المريرة للانتخابات في مواجهة نائبه، آل جور، والتي انتهت بفوز بوش فقط بعد أن أوقفت المحكمة العليا إعادة فرز الأصوات في ولاية فلوريدا.

ألقى بوش بالكثير من مبادرات كلينتون، من بينها تلك التي لها علاقة بالأمن السيبراني. ظل كلارك، مهندس تلك السياسات، باقيا في البيت الأبيض، واحتفظ بمنصب «المنسق القومي لشؤون الأمن، وحماية البنية الأساسية، ومكافحة الإرهاب». لكن بات جليا أن بوش لم يكن يهتم بشأن أي من هذه القضايا، وكذلك كان نائبه ديك تشيني Dick Cheney أو كوندوليزا رايس Condoleezza Rice مستشار الرئيس للأمن القومي. في عهد كلينتون، كان كلارك يتمتع بمكانة أمين مجلس الوزراء، حتى إن لم يكن ذلك على نحو رسمي، وكان يشارك في اجتماعات مجلس الأمن القومي - الذي كان يحضره وزراء الدفاع، والخارجية، والخزانة، وغيرها من الوزارات - حينما كانوا يناقشون القضايا التي كان يتولاها. سلبته رايس ذلك الامتياز. لم يفسر كلارك هذه الخطوة على أنها إهانة شخصية فقط، بل على أنها انتقاص من شأن قضاياه.

في أثناء الأشهر القليلة الأولى من فترة ولاية بوش[19]، حذَّر كلارك وجورج تينيت George Tenet، مدير وكالة الاستخبارات المركزية، وهو أيضا من بقايا نظام كلينتون، الرئيس مرارا وتكرارا بشأن الخطر الوشيك المتمثل في اعتداء على أمريكا سيشنه أسامة بن لادن. لكن بوش نحى تلك التحذيرات جانبا. كان بوش ومستشاروه المقربون أكثر قلقا بشأن تهديدات صواريخ من روسيا، وإيران، وكوريا الشمالية، وكان على رأس أولوياتهم إلغاء معاهدة الحد من المنظومات المضادة للقذائف التسيارية (الباليستية) التي مضى عليها ثلاثون عاما، وهي الاتفاقية السوفييتية الأمريكية التي كانت تمثل علامة بارزة في الحد من التسلح، ومن ثم كان سيمكنهم بناء نظام دفاع صاروخي. (في يوم هجمات الحادي عشر من سبتمبر[20]، كان من المخطط أن تلقي رايس خطابا بشأن التهديدات الرئيسية التي تواجه البر، لم تكن مسودة الخطاب تتضمن ما يشير إلى بن لادن أو تنظيم القاعدة).

في يونيو من العام 2001، قدم كلارك استقالته. كان كلارك هو كبير مستشاري البيت الأبيض لمكافحة الإرهاب، ومع ذلك لم يكن أحد يهتم بالإرهاب أو به. فوجئت رايس، وألحت عليه وحثته على ألا يغادر. خضع كلارك، موافقا على البقاء ولكن فقط إذا اقتصرت مسؤولياته على الأمن السيبراني، ومنحه هيئة موظفين خاصة به (في نهاية المطاف بلغ عددهم ثمانية عشر)، والسماح له بتشكيل وإدارة مجلس سيبراني مشترك بين الوكالات. وافقت رايس، لأنها من ناحية لم تكن تعبأ كثيرا بشأن السيبرانية، وكانت ترى منحه هذا الامتياز على أنه وسيلة لإبقاء كلارك موجودا مع إبقائه بعيدا عن القضايا التي تقع في دائرة اهتماماتها. مع ذلك، كانت رايس في حاجة إلى وقت لتجد بديلا لموضع مكافحة الإرهاب الشاغر، لذلك وافق كلارك على البقاء في هذا المنصب حتى الأول من أكتوبر.

حينما صدمت الطائرات المخطوفة مركز التجارة العالمي ومقر البنتاغون، كان كلارك قبل رحيله لايزال لديه بضعة أسابيع باعتباره مسؤولا عن مكافحة الإرهاب. كان بوش في فلوريدا، وعلى عجل أُخذ تشيني إلى مخبأ تحت الأرض؛ واعتياديا، جلس كلارك في غرفة العمليات بوصفه مديرا للأزمة، يدير المؤتمرات الهاتفية المشتركة بين الوكالات، وينسّق، وفي بعض الحالات يوجّه، رد الحكومة وتحركها.

عززت التجربة مكانته بعض الشيء، ليس بالقدر الكافي للسماح له بالعودة إلى اجتماعات كبار المسؤولين، ولكن بما يكفي لأن يبدأ قليل من الاهتمام بالأمن السيبراني. على الرغم من ذلك، أحجمت رايس حينما اقترح كلارك تجديد الخطة القومية لحماية نظم المعلومات، التي كان قد كتبها إلى كلينتون في العام الأخير من فترته الرئاسية. تذكرت رايس على نحو غير واضح أن الخطة كانت تضع معايير إلزامية للقطاع الخاص، وأن ذلك سيكون شيئا بغيضا بالنسبة إلى الرئيس بوش.

في الواقع، وبقدر ما كان كلارك يتمنى أن تكون كذلك، فإن الخطة في إصدارها المعدل، بعد أن اضطر كلارك إلى التخلي عن اقتراحه الخاص بالشبكة الفدرالية لكشف التسلل، لم تكن تدعو إلا إلى التعاون بين القطاعين العام والخاص، مع وجود الشركات في موضع القيادة. لكن كلارك كان يجاري رايس، متفقا معها على أن خطة كلينتون كانت معيبة إلى حد كبير، وأنه كان يرغب في إعادة كتابتها على نحو جذري. دعته رايس يعد مسودة لأمر تنفيذي يدعو إلى خطة جديدة[21]، ووقع بوش على الأمر التنفيذي في 30 سبتمبر. طوال الأشهر القليلة اللاحقة، مضى كلارك وبعض موظفيه في طريقهم، وعملوا على أن يعقد البيت الأبيض «لقاءات عامة سيبرانية» في دور البلدية في عشر مدن، شملت: بوسطن Boston، ونيويورك New York، وفيلادلفيا Philadelphia، وأتلانتا Atlanta، وسان فرانسيسكو San Francisco، ولوس أنجلوس Los Angeles، وبورتلاند Portland، وأوستن Austin، ودعوا إليها خبراء محليين، ومسؤولين تنفيذيين في الشركات، ومديري تكنولوجيا المعلومات، ومسؤولي إنفاذ القانون.

كان كلارك يبدأ الجلسات بتعليق متواضع. كان يقول، بعضكم انتقد خطة كلينتون لأنه لم يكن لكم أي إسهام فيها. واستطرد كلارك: الآن كانت إدارة بوش تكتب خطة جديدة، والرئيس يريد منكم، أنتم الأناس المتأثرين بمحتواها، يريد منكم أن تكتبوا الملاحق التي تتناول قطاعكم للبنية الأساسية الحرجة. في بعض المدن، كان بعض الخبراء والمديرين التنفيذيين بالفعل يقدمون أفكارا، وكان قطاع الاتصالات متحمسا على نحو خاص.

بيد أن واقع الأمر تمثل في أن كلارك لم يكن مهتما بأفكارهم. مع ذلك، فهو كان يرغب في إذابة معارضتهم. كان المغزى الأساسي والوحيد من التمثيليات المسرحية في

اللقاءات العامة في دور البلدية، هو الحصول على تأييدهم من أجل استمالتهم نحو الاعتقاد بأنه كان لديهم ما يقدمونه حيال التقرير. وكما تبين، فإن المسودة النهائية[22] - وهي وثيقة مؤلفة من ستين صفحة كانت تسمى «الاستراتيجية القومية لحماية الفضاء السيبراني» The National Strategy to Secure Cyberspace، التي وقّعها الرئيس بوش في 14 فبراير من العام 2003 - كانت تحتوي على مزيد من المقاطع التي تتملق الصناعة وتذعن لها، وكانت تعهد إلى وزارة الأمن الداخلي الجديدة ببعض من مسؤولية تأمين الفضاء السيبراني غير العسكري. لكن بخلاف ذلك، فإن الصياغة اللغوية المتعلقة بأوجه الضعف والثغرات الأمنية لأجهزة الحاسوب، جاءت مباشرة من تقرير مارش، وكانت الأفكار بشأن ما يجب فعله حيال ذلك مطابقة تقريبا للخطة التي كان كلارك قد كتبها إلى كلينتون.

وضعت الوثيقة إطارا عن الكيفية التي سيكون عليها التعامل مع الأمن السيبراني على مدار الأعوام القليلة اللاحقة، وكذلك محدودية مقدرة الحكومة على أن تتكفل بالأمر برمته، في ضوء معارضة الصناعة للمعايير الإلزامية وأوجه قصور الجهاز الإداري والتقني في وزارة الأمن الداخلي (مشكلة كانت ستصير جلية قريبا).

لم ينتظر كلارك ليجابه المعارك السياسية المتعلقة بتنقيح الخطة الجديدة وإنفاذها. في 19 مارس، أمر بوش بغزو العراق. في أثناء الحشد استعدادا للحرب، كان كلارك قد دفع بحجة مُفادها أن الحرب كانت ستحول الاهتمام والموارد عن المعركة ضد بن لادن وتنظيم القاعدة. حالما تأكد بدء تروس آلة الحرب في الحركة، استقال كلارك محتجا.

لكن بعد بضعة أعوام من الغزو، وبينما كانت الحرب تنتقل من التحرير إلى الاحتلال، والعدو يتحول من صدام حسين إلى صفيف متباين من المتمردين، كان المحاربون السيبرانيون في «فورت ميد» والبنتاغون يدخلون إلى ساحة المعركة للمرة الأولى باعتبارهم قوة مهمة لا يستهان بها، بل حتى قوة حاسمة.

9

حروب سيبرانية

«كان بإمكانه رؤية «درجات السلم الحبل» للجهاديين الأجانب الذين يتسللون إلى العراق عبر سورية، وقراءة نصوص محادثاتهم الهاتفية التي تُضاهى مع خرائط تبين مواقعهم بدقة».

حينمـــا تولى الجنرال جون أبي زيد[1] John Abizaid زمام القيادة المركزية للولايات المتحدة في 7 يوليو من العام 2003، مشرفا على العمليات العسكرية الأمريكية في الشرق الأوسط وآسيا الوسطى وشمال أفريقيا، كانت القيادة السياسية في واشنطن تظن أن الحرب في العراق قد انتهت. أخيرا، كان الجيش العراقي قد دُحر، وكان صدام حسين قد لاذ بالفرار، وكان النظام البعثي قد انهار. لكن أبي زيد كان يعرف أن الحرب كانت قد بدأت، وكان حائرا لأن الرئيس بوش وكبار مسؤوليه لم يستوعبوا طبيعة تلك الحرب، ولم يمنحوه الأدوات اللازمة لخوضها. كانت السيبرانية هي إحدى تلك الأدوات.

تدرج أبي زيد في سلم المناصب في صفوف الجيش الميداني (القوات البرية) في سلاح المشاة المحمولة جوا، وبعثات الأمم المتحدة لحفظ

السلام، ووظائف المراتب العليا في البنتاغون. لكن في بدايات حياته المهنية عاش أبي زيد تجربة غير تقليدية. في منتصف الثمانينيات من القرن العشرين، بعد خدمته قائد سرية في معركة «غرينادا» Grenada القصيرة، أُسنِدت إليه «مجموعة دراسات الجيش الميداني»، التي كانت تستكشف مستقبل الحرب. كان نائب رئيس أركان الجيش الميداني الجنرال ماكس ثورمان Max Thurman، مفتونا بتقارير بشأن أبحاث الجيش السوفييتي في مجال الاستشعار من بعد والتجارب النفسية. إنها لم تسفِر عن شيء، لكنها جعلت أبي زيد يتعرض لفكرة أنه من الممكن أن تكون الحرب أكثر من مجرد رصاصات وقنابل.

في منصبه اللاحق مساعدا تنفيذيا للجنرال جون شاليكاشفيلي John Shalikashvili، رئيس الهيئة المشتركة لرؤساء الأركان، رافق أبي زيد رئيسه ذات مرة في رحلة إلى موسكو Moscow. هناك أدركوا أن غرفهم بها أجهزة تنصت، فأعدّ طاقم العاملين خياما صغيرة حتى يتمكنوا من مناقشة أعمالهم الرسمية بعيدا عن تنصت الروس. في وقت لاحق في البوسنة Bosnia، بوصفه قائدا مساعدا للفرقة الأولى المدرعة، علِم أبي زيد أن وكالة الاستخبارات المركزية كانت تطلق طائرات استطلاع من دون طيار فوق سراييفو Sarajevo، وهو كان على عِلم بقلق مسؤولي استخبارات الولايات المتحدة على الأرض، من احتمال أن يسيطر الروس على إحدى الطائرات من خلال اختراق وصلة الاتصالات الخاصة بها.

بحلول العام 2001، حينما رُقِّي أبي زيد ليصير مدير هيئة الأركان المشتركة في البنتاغون، كانت خطط وبرامج الأمن السيبراني ووسائل الحرب السيبرانية في أوج ازدهارها. وضعته وظيفته وسط المهاترات والخلافات الشائكة والمكائد داخل فروع القوات المسلحة، وبين بعضها وبعض؛ لذلك، كان أبي زيد يعرف جيدا التوترات بين القائمين بالعمليات والجواسيس في مختلف مناحي المجال السيبراني. في حالة نشوب الحرب كان مسؤولو العمليات، وبشكل رئيسي في الفروع العسكرية، سيرغبون في استخدام المعلومات الاستخباراتية التي يُحصَل عليها بالأساليب السيبرانية. أما الجواسيس، بشكل أساسي في وكالة الأمن القومي ووكالة الاستخبارات المركزية، فكانوا يرون المعلومات الاستخباراتية على أنها في حد ذاتها حيوية وبالغة الأهمية، وكانوا يخشون أن استخدامها كان سيعني فقدانها،

لأن العدو كان سيعرف أننا كنا نخترق شبكاته، لذا كانوا سيغيرون رموز شفرتهم أو سيقيمون موانع جديدة. فهم أبي زيد هذا التوتر - إنه كان عنصرا طبيعيا في السياسات العسكرية - لكن أبي زيد كان في الأساس رجل عمليات. ذهب أبي زيد بجولة إرشادية في «فورت ميد»، وكان منبهرا بالعجائب التي كانت وكالة الأمن القومي تستطيع تحقيقها، وكان يعتقد أنه سيكون من الجنون إنكار فضلهم على الجنود الأمريكيين في المعركة.

في الفترة التي سبقت غزو العراق كان أبي زيد قد أصبح نائبا لرئيس القيادة المركزية، طار أبي زيد إلى مقر القيادة الفضائية في «كولورادو سبرينغز»، مقر «فريق العمل المشترك لعمليات شبكة الحاسوب»، الذي كان من الناحية النظرية سيقود الهجوم والدفاع السيبراني في وقت الحرب. لقد هاله مدى الصعوبة الإدارية التي كانت ستواجه حشد أي نوع من الحملات الهجومية السيبرانية؛ لشيء واحد، كانت أدوات الهجوم السيبراني والتجسس السيبراني تكتنفها السرية إلى درجة أنه حتى وجودها لا يعرف به سوى عدد من القادة العسكريين.

سأل أبي زيد الميجور جنرال (اللواء) جيمس د. بريان James D. Bryan، رئيس فريق العمل المشترك، كيف كان سيحصل على معلومات استخباراتية من حواسيب تنظيم القاعدة لتصل إلى أيدي الجنود الأمريكيين في أفغانستان. تتبع بريان التسلسل القيادي المتشابك الملتوي، من القيادة الفضائية إلى جماعة من الجنرالات في البنتاغون، وصولا إلى نائب وزير الدفاع، ثم وزير الدفاع، إلى مجلس الأمن القومي في البيت الأبيض، وفي نهاية المطاف إلى الرئيس. حينما يكون الطلب قد تخطى كل هذه الحواجز، من المحتمل أن حاجة الجنود إلى المعلومات الاستخباراتية ستكون قد انتفت، وربما تكون الحرب ذاتها انتهت.

في 19 مارس أمر بوش بغزو العراق. بعد مضي ثلاثة أسابيع، وبعد هجوم مدرع خاطف عبر الصحراء من جهة الكويت، سقطت بغداد. في يوم عيد العمال (الأول من مايو)، وبعد ثلاثة أسابيع من الإطاحة وقف الرئيس بوش على سطح حاملة الطائرات الأمريكية أبراهام لنكولن Abraham Lincoln، أسفل لافتة كتب عليها «تم إنجاز المهمة» (Mission Accomplished)، وأعلن انتهاء العمليات القتالية الرئيسية. لكن في وقت لاحق من ذلك الشهر، أصدر الحاكم الأمريكي،

بول بريمر L. Paul Bremer، توجيهين: تسريح الجيش العراقي، وحرمان أعضاء حزب البعث من تولي السلطة. أدت تلك الأوامر إلى شعور السكان السنة بالامتعاض الشديد، لدرجة أنه مع تولي أبي زيد منصب قائد القيادة المركزية، اندلع عصيان مستعر غاضب ضد الحكومة العراقية الجديدة التي يقودها الشيعة وضد حُماتها الأمريكيين.

سمِع أبي زيد بشأن الكم الهائل من المعلومات الاستخباراتية الآتية من العراق: اعتراضات اتصالات، وبيانات نظام تحديد المواقع (نظام التموضع العالمي) Global Positioning System (GPS) من هواتف المتمردين الجوالة، وصور أقمار اصطناعية للجهاديين السنة يتدفقون عبر الحدود السورية؛ لكن لم يكن هناك أحد يجمع تلك العناصر معا، فضلا عن إدراجها ودمجها في خطة عسكرية. كان أبي زيد يرغب في أن يدخل إلى تلك الاعتراضات ويرسل إلى المتمردين رسائل مزيفة، موجها إياهم إلى موقع معين، حيث ستكون قوات العمليات الخاصة الأمريكية راقدة في انتظارهم لتقتلهم وتقضي عليهم. لكنه كان بحاجة إلى تعاون وكالة الأمن القومي ووكالة الاستخبارات المركزية لتجدل هذه المعلومات الاستخباراتية معا، وكان بحاجة إلى موافقة القيادة السياسية على استخدامها باعتبارها إحدى الأدوات الهجومية. في تلك اللحظة لم يكن لديه أي منهما.

لم تكن الأجهزة الإدارية الراسخة في «لانغلي» و«فورت ميد» ترغب في التعاون، وكانوا يعرفون أن العالم، بمن في ذلك الروس والصينيون، كان يراقب المشهد، وهم لم يرغبوا في تبديد أفضل ما لديهم من تقنيات جمع المعلومات الاستخبارية في حرب يرى الكثيرون أنها غير ضرورية. في الوقت نفسه فإن وزير الدفاع دونالد رامسفيلد Donald Rumsfeld[2] لم يكن ليعترف بوجود تمرد. (كان رامسفيلد قديما بما يكفي - من أيام حرب فيتنام - لأن يعرف أن هزيمة التمرد تتطلب استراتيجية مضادة للتمرد، التي بدورها كانت ستتطلب ترك عشرات الآلاف من جنود الولايات المتحدة في العراق طوال أعوام، وربما عقود، في حين لم يكن يريد سوى الدخول، والخروج، والانتقال إلى طرد الطاغية التالي الذي يقف في طريق الهيمنة الأمريكية على ما بعد الحرب الباردة).

بسبب الإحباط وخيبة الأمل تحول أبي زيد إلى جنرال ذي نجمة واحدة يدعى كيث ألكسندرKeith Alexander. كان الاثنان قد تخرجا في «ويست

بوينت» West Point[*] يفصل بينهما عام واحد – تخرج أبي زيد في العام 1973، وألكسندر في العام 1974- وبعد ذلك بنحو عشرين عاما، كانا قد التقيا مجددا فترة وجيزة في أثناء تدريب قيادة الكتيبة في إيطاليا. كان ألكسندر قد أصبح مسؤولا عن «قيادة استخبارات وأمن الجيش الميداني» في «فورت بيلفوار» Fort Belvoir بولاية فيرجينيا Virginia، وهي مركز استخبارات الإشارة (سيجينت) الخاص بالقوات البرية، يحوي 11 ألف ضابط استطلاع منتشرين في كل أرجاء العالم، كان في حد ذاته وكالة أمن قومي مصغرة، ولكن تُوجَّه صراحة إلى مهام الجيش الميداني. ربما كان بمقدور ألكسندر أن يساعد أبي زيد على إضفاء لمحة عملياتية على البيانات الاستخباراتية.

كان أبي زيد قد جاء إلى الرجل المناسب. كان ألكسندر بمنزلة مرشد تقني. في السابق في «ويست بوينت»، كان ألكسندر يعمل على حواسيب قسم الهندسة الكهربائية وقسم الفيزياء. في أوائل الثمانينيات من القرن العشرين، في «مدرسة الدراسات العليا البحرية» في مدينة مونتيري Monterey بولاية كاليفورنيا California، بنى ألكسندر حاسوبا خاصا به، واستحدث برنامجا لتعليم أفراد الجيش الميداني كيفية التحول من بطاقات الفهرسة المكتوبة بخط اليد إلى قواعد البيانات المؤللة. بعد تخرجه بوقت قصير عُيِّن في «مركز استخبارات الجيش الميداني» في «فورت هواتشوكا» Fort Huachuca بولاية أريزونا Arizona، حيث أمضى أول عطلة لنهاية الأسبوع في حِفظ المواصفات الفنية لجميع حواسيب الجيش الميداني، ثم أعد خطة رئيسية لجميع أنظمة البيانات المتعلقة بالاستخبارات ووسائل الحرب الإلكترونية. في أثناء الاستعداد لعملية «عاصفة الصحراء» - حرب الخليج الأولى في العام 1991 - قاد ألكسندر إحدى الجماعات في الفرقة الأولى المدرعة في «فورت هود» بولاية تكساس Texas، ووصَّل مجموعة من أجهزة الحاسوب سلكيا معا ليمكنها معالجة البيانات على نحو أكثر كفاءة. وبدلا من الاعتماد على المخرجات

(*) «ويست بوينت» West Point: هي الأكاديمية العسكرية الأمريكية، وتسمى «ويست بوينت» نسبة إلى المنطقة التي توجد بها في ولاية نيويورك، وهي مؤسسة فدرالية أمريكية تختص بتدريس العلوم العسكرية للرجال والنساء على حد سواء، ومدة الدراسة بها أربع سنوات، وهي الأقدم بين الأكاديميات العسكرية الأمريكية الخمس؛ إذ تأسست في العام 1802.

المطبوعة والفهرسة اليدوية، كان بإمكان المحللين ومخططي الحرب في البنتاغون الوصول إلى البيانات التي خُزِّنت، وفرزها وفقا لاحتياجاتهم.

قبل أن يتولى ألكسندر منصبه القيادي الحالي في «فورت بيلفوار» كان كبير ضباط الاستخبارات في القيادة المركزية. وقد أخبر أبي زيد بشأن طفرة التطورات التقنية على الساحة، وأبرزها الأدوات التي يمكن أن تعترض الإشارات الصادرة عن رقائق الهواتف الجوالة، إما مباشرة أو من خلال عقد التبديل في شبكة الاتصالات الجوالة، مما يسمح لفرق استخبارات الإشارة بتتبع موقع مقاتلي «طالبان» وتحركاتهم في الحدود الشمالية الغربية لباكستان أو المتمردين في العراق - حتى إن كانت هواتفهم مغلقة. كان هذا سلاحا جديدا في الترسانة السيبرانية، ولم يكن أحد قد استغل إمكاناته بعد، فضلا عن وضع إجراءات لتشارك إحدى الدوائر ما لديها من معلومات استخباراتية مع دوائر أخرى، أو مع قادة في الميدان. كان أبي زيد حريصا على أن يمضي أسلوب التشارك هذا قدما.

على الرغم من أن القيادة المركزية كانت تشرف على العمليات العسكرية الأمريكية في العراق، وأفغانستان، والدول المجاورة لهما، فإن مقرها الرئيسي كان في مدينة تامبا Tampa بولاية فلوريدا Florida؛ لذلك، كان أبي زيد يذهب في رحلات متكررة إلى واشنطن Washington. بحلول شهر أغسطس، بعد شهر واحد من تولي أبي زيد منصبه قائدا لها، كانت المعلومات الاستخباراتية بشأن المتمردين تتدفق إلى «لانغلي» و«فورت ميد». كان بإمكانه رؤية «درجات السلم الحبل» للجهاديين الأجانب الذين يتسللون إلى العراق عبر الحدود السورية، وقراءة نصوص محادثاتهم الهاتفية التي تُضَاهَى مع خرائط تبين مواقعهم بدقة. كان أبي زيد يرغب في أن يمنح الجنودَ الأمريكيين إمكانية الوصول إلى هذه المعلومات الاستخباراتية، حتى يمكنهم استخدامها في ساحة المعركة.

بحلول ذلك الوقت كان كيث ألكسندر قد رُقِّي ليشغل منصب نائب رئيس أركان الجيش الميداني لشؤون الاستخبارات داخل البنتاغون، لذلك تعاون هو وأبي زيد في العمل على القضايا الجوهرية والسياسات الإدارية. وجدا داعما مثاليا في الجنرال ستانلي ماكريستال Stanley McChrystal، رئيس قيادة العمليات الخاصة المشتركة. إذا شق هذا الكنز الجديد من المعلومات الاستخباراتية طريقه إلى القوات

الموجودة في الميدان فإن جنود الظل (الطابور الخامس) في قيادة العمليات الخاصة المشتركة سيكونون هم أول جنود يحصلون عليها ويستخدمونها، وكان ماكريستال جنديا شجاعا مِقداما، حريصا على تحقيق ذلك. أدخل الثلاثة وجهة نظرهم إلى البنتاغون ودوائر الاستخبارات، لكن العقبة الرئيسية كانت رامسفيلد، الذي كان لايزال يرفض اعتبار الثوار العراقيين متمردين.

في نهاية المطاف، في يناير من العام 2004، رتّب أبي زيد لاجتماع مع الرئيس بوش حيث قدم له مسوغات إطلاق العمليات الهجومية السيبرانية ضد المتمردين. طلب بوش من مستشاره للأمن القومي، كوندوليزا رايس، وضع الموضوع على جدول أعمال اجتماع مجلس الأمن القومي المقبل. حينما طُرِح الموضوع بعد عدة أيام لاحقة، أسقطه نواب دوائر الاستخبارات بحجة قديمة، وهي أن الاعتراضات كانت تقدم معلومات ممتازة بشأن المتمردين، والهجوم على مصدر المعلومات كان من شأنه تنبيههم لأنهم كانوا يتعرضون للاختراق (هم وأعداء آخرون محتملون ربما يكونون قيد المراقبة)، الأمر الذي سيدفعهم إلى تغيير رموز شفرتهم، أو إلقاء هواتفهم الجوالة، مما يؤدي إلى خسارة استخباراتية جسيمة.

في أثناء ذلك كان المتمردون العراقيون يزدادون قوة، وكانت أمريكا تخسر الحرب، وبدأ بوش يفقد صبره. مذعورا من المقاومة لمناهج جديدة، ومتشككا في أن جيشا خارجيا كان يمكنه تصحيح الأمور في العراق بأي طريقة، تحرك أبي زيد نحو الرأي القائل إنه كان على الولايات المتحدة أن تبدأ في الخروج، بدلا من مضاعفة جهودها.

لكن الأمور بدأت تتغير بعد ذلك. بعد أن ضاق رامسفيلد ذرعا واستاء من كل كبار جنرالات الجيش الميداني تخطى قائمة المرشحين لمنصب رئيس هيئة أركان الجيش الميداني الشاغر، واستدعى الجنرال بيتر سكوومیكر Peter Schoomaker من التقاعد.

كان سكوومیكر قد أمضى معظم حياته المهنية في القوات الخاصة، وكانت تلك صفعة أخرى على وجه الجيش الميداني الاعتيادي. (كان الجنرال نورمان شوارتسكوف Norman Schwarzkopf، بطل عاصفة الصحراء، قد تحدث إلى الكثير من أقرانه حينما كان يتهكم على القوات الخاصة بوصفهم «أكلة ثعابين» منفلتين وخارجين

عن السيطرة). أخبره ماكريستال، الذي كان قد عرف سكووميكر منذ وقت طويل وكان يبجله ويحترمه، أخبره بالأفكار التي كان هو، وأبي زيد، وألكسندر قد جاهدوا لتمريرها. وجد الرئيس الجديد تلك الأفكار جذابة، لكنه أدرك أنهم كانوا بحاجة إلى مناصر رفيع المستوى في الأوساط الاستخباراتية. في بداية العام 2005 كان مايك هايدن يقترب من نهاية فترة ولايته مديرا لوكالة الأمن القومي التي على نحو استثنائي طالت إلى ستة أعوام. حث سكووميكر رامسفيلد على أن يحل ألكسندر محل هايدن.

كانت سبعة عشر عاما قد مرت[3] منذ أن كان ضابط من الجيش الميداني قد تولى إدارة وكالة الأمن القومي. عبر تاريخ الوكالة الذي يمتد إلى خمسة وثلاثين عاما، لم يتول إداراتها من جنرالات الجيش الميداني سوى ثلاثة فقط، مقارنة بسبعة جنرالات من سلاح الجو، وخمسة أدميرالات من سلاح البحرية. كان هذا النمط قد عكس، وعزز، ممانعة الوكالة لتشارك المعلومات الاستخباراتية مع القادة الميدانيين الذين يخوضون «حروبا صغيرة»، وهم عادة ما يكونون من ضباط الجيش الميداني. لكن حينذاك كانت الولايات المتحدة تخوض حربا صغيرة، اعتبرها الرئيس الحالي أمرا جللا. كالعادة كان الجيش الميداني هو الذي يتحمل العبء الأكبر من الضحايا، وخطط ألكسندر لاستخدام منصبه الجديد للمساعدة على قلب النزاع وتبديل الأمر.

كان ماكريستال قد حقق بالفعل طفرات وإنجازات غير مسبوقة في جمع مسارات المعلومات الاستخباراتية المتباينة وجدْلِها معا. وكان قد تولى رئاسة «قيادة العمليات الخاصة المشتركة» في سبتمبر من العام 2003. وفي الشهر نفسه، وقّع رامسفيلد[4] أمرا تنفيذيا يخول قيادة العمليات الخاصة المشتركة تنفيذ عمل عسكري ضد تنظيم «القاعدة» في أي مكان في العالم من دون موافقة مسبقة من الرئيس أو إخطار الكونغرس. لكن ماكريستال وجد نفسه غير قادر على تنفيذ الكثير مع هذا التسريب للقوة الكبرى، إذ كان رؤساء الأركان في البنتاغون معزولين عن قيادات العمليات القتالية، وكان قادة العمليات القتالية معزولين عن دوائر الاستخبارات. كان ماكريستال يرى تنظيم «القاعدة» على أنه شبكة، قوة كل خلية تعززها روابطها وعلاقاتها بالخلايا الأخرى. كان الأمر سيتطلب شبكة لمحاربة شبكة، وشرع ماكريستال في بناء شبكته الخاصة، وتواصل مع وكالة الاستخبارات المركزية،

ومكاتب الاستخبارات المنفصلة في الفروع العسكرية، والوكالة القومية للاستخبارات الجغرافية المكانية (الجيومكانية)، وضباط الاستخبارات في القيادة المركزية. استحثهم على إبرام اتفاقيات لتشارك البيانات، وصور الأقمار الاصطناعية، والطائرات من دون طيار، واعتراضات الهاتف الجوال، وعمليات التنصت على خطوط الهاتف الأرضي. (حينما أعادت إدارة بوش بناء نظام الهاتف العراقي بعد الإطاحة بـ «صدام»، سُمِح لوكالة الاستخبارات المركزية ووكالة الأمن القومي بالدخول لوضع بعض الأجهزة). لكن لتحقيق ذلك – لصهر كل هذه المعلومات في قاعدة بيانات مترابطة ومتناسقة وتحويلها إلى سلاح هجومي – كان ماكريستال يحتاج أيضا إلى الأدوات التحليلية وتكنولوجيا المراقبة الموجودة لدى وكالة الأمن القومي.

هنا جاء دور ألكسندر.

حينما تولى كيث ألكسندر رئاسة «فورت ميد»، في الأول من أغسطس من العام 2005، تنحى سلفه مايك هايدن غاضبا ومكتويا بنيران الريبة.

قبل ذلك ببضعة أعوام، حينما كان ألكسندر[5] يدير «قيادة استخبارات وأمن الجيش الميداني» في «فورت بيلفوار»، كان كل من الرجلين قد اصطدم بالآخر في صراع مطرد من أجل النفوذ والسلطة، مخلِّفا هايدن بمرارة في حلقه، وبدنا مقشعرا ومرتعدا من الريبة بشأن كل وجهة ونشاط للرجل الجديد المسؤول.

منذ اللحظة التي تولى فيها ألكسندر القيادة في «فورت بيلفوار» كان عازما على تحويل المكان من مركز إداري، مكلف على نحو ضيق بتقديم استخبارات الإشارة إلى وحدات الجيش الميداني، وخاضع لكل من رئيس أركان الجيش الميداني ومدير وكالة الأمن القومي؛ إلى قيادة ند مماثِلة، تشارك في العمليات، لاسيما في الحرب على الإرهاب.

في منصبه السابق رئيسا لاستخبارات القيادة المركزية كان ألكسندر قد ساعد على تطوير أدوات تحليلية جديدة عالجت كميات هائلة من البيانات، وحللت محارفها بحثا عن أنماط وعلاقات. فكر ألكسندر في أن تقنية تتبع روابط الهاتف والبريد الإلكتروني («أ» كان يتحدث إلى «ب»، الذي كان يتحدث إلى «ج»، وهكذا)، كان يمكن أن تساعد على تعقب الإرهابيين وكشف شبكاتهم. كان يمكن أن تكون بمنزلة مدخل لألكسندر إلى الفئة العليا في عالم الاستخبارات.

لكن ألكسندر كان يحتاج إلى تغذية برمجيته بالبيانات، وكانت البيانات لدى وكالة الأمن القومي. طلب ألكسندر من هايدن أن يتشارك البيانات، لكن هايدن خذله ورفض. كانت قواعد البيانات هي جواهر التاج بالنسبة إلى الوكالة، وهي نتاج عقود من الاستثمارات في تكنولوجيا جمع البيانات، والحواسيب، والثروة البشرية. لكن ممانعة هايدن لم تكن مسألة حماية الحِمى والنفوذ فقط. طوال أعوام كانت دوائر استخبارات أخرى قد سعت إلى الوصول إلى قاعدة بيانات «فورت ميد»، من أجل إجراء تجربة ما أو للمضي في جدول الأعمال الخاصة بهم. لكن تحليل استخبارات الإشارة كان تخصصا مقصورا على فئة قليلة، كان يمكن أن يتولد من البيانات الخام استنتاجات خاطئة، أو حتى خطيرة، إذا وضعت في أيد غير مدربة، وما كان ألكسندر يريد فعله بالبيانات - «تحليل حركة البيانات» كما أطلقت عليه وكالة الأمن القومي - كان على نحو خاص عرضة لهذا الجنوح. إن المصادفات لا تكون دليلا على السببية، نقطة اتصال مشتركة - على سبيل المثال، رقم هاتف تصادف أن اتصل به بضعة أشخاص مشتبه فيهم - لا يكون دليلا على وجود شبكة، فضلا على كونها مؤامرة.

كان لدى «فورت بيلفوار» سجل رديء جدا في درء هذه الأنواع تحديدا من العلاقات المهلهلة. في العام 1999، قبل عامين من وصول ألكسندر، كان سلفه، الميجور جنرال (اللواء) روبرت نونان Robert Noonan، قد أنشأ مكتبا خاصا أطلق عليه اسم «نشاط وسائل حرب المعلومات البرية»، وبعد فترة وجيزة تغير اسمه إلى «مركز الهيمنة المعلوماتية». كانت إحدى تجاربه هي معرفة ما إذا كان يمكن لبرنامج حاسوبي أن يكتشف تلقائيا أنماطا في البيانات على الإنترنت - تحديدا أنماطا تدل على نفاذ أجنبي غريب إلى برامج البحث والتطوير الأمريكية.

كان آرت موني، مساعد وزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات، قد موَّل التجربة، وحينما تم الانتهاء منها، ذهب هو وجون هامري، نائب وزير الدفاع، إلى «فورت بيلفوار» لحضور جلسة إحاطة. عرض نونان مجموعة كبيرة من الصور والرسوم البيانية، التي تبين الرئيس كلينتون، ووزير الدفاع السابق وليام بيري William Perry، وبيل غيتس Bill Gates، الرئيس التنفيذي لشركة

مايكروسوفت، ومعهم مسؤولون صينيون، بدا أن الاستنتاج كان أن الصين قد تغلغلت في أعلى مستويات الحكومة والصناعة الأمريكية.

كان هامري غاضبا مستاء، لاسيما أن الإحاطة كانت قد عُرضت بالفعل لعدد من الجمهوريين في الكونغرس. حاول نونان أن يدافع عن البرنامج قائلا إنه لم يقصد به تحليلا استخباراتيا، بل نوعا من مشروعات معرض العلوم الذي يظهر إمكانات التكنولوجيا. لم يجد هامري الأمر مسليا ولم يرقه، وأغلق المشروع.

كان مهندس المشروع والمصمم الرئيسي له هو كبير مستشاري التكنولوجيا في «بيلفوار»، وهو مهندس غير عسكري يدعى جيمس هيث James Heath، حاد، واثق بنفسه، انطوائي جدا (حينما كان يتحدث مع الزملاء، لم يكن فقط يطأطئ رأسه ناظرا إلى أحذيتهم، بل كان يطأطئ رأسه ناظرا إلى حذائه هو)، كان هيث متعصبا بشأن إمكانات تتبع الروابط والعلاقات في البيانات الضخمة big data - على وجه التحديد - ما كان سيطلق عليه في وقت لاحق «البيانات الواصفة» metadata.

ربما كان نقد هامري اللاذع يعني نهاية الحياة المهنية للبعض، لكن هيث بقي في مكانه، وحينما تولى ألكسندر قيادة «فورت بيلفوار»، في أوائل العام 2001، تبدلت حظوظه. كان كل منهما قد عرف الآخر منذ منتصف التسعينيات من القرن العشرين، حينما كان ألكسندر قائد اللواء الرقم 525 للاستخبارات العسكرية في «فورت براغ» بولاية كارولينا الشمالية North Carolina، وكان هيث هو مستشاره العلمي. حتى ذلك الحين، كانا يعملان على برمجيات «التجسيد المرئي للبيانات» (data visualization)، وكان ألكسندر معجبا بفطنة هيث وعقليته المتفردة. كان زملاء هيث في العمل، حتى المقربون منه، يشيرون إليه على أنه «العالم المجنون» الذي يخص ألكسندر.

إحدى مخاوف مايك هايدن بشأن طلب ألكسندر بيانات وكالة الأمن القومي الخام، كانت أن هيث هو الذي كان سيعمل على البيانات. كان هذا سببا آخر لرفض هايدن الطلب.

لكن ألكسندر كافح وقاوم. كان لطيفا معسول اللسان، ووسيما جذابا، وحتى فكها يتمتع بروح الدعابة بأسلوب أخرق يخفي طموحه العدواني، شن حملة

ضغط كبيرة لكسب التأييد ليحصل على البيانات. كان ألكسندر يخبر أي شخص، وكل شخص لديه أي سلطة أو نفوذ، لاسيما في «الكابيتول هيل» وفي البنتاغون، بأنه هو وفريقه في «فورت بيلفوار» استحدثوا برمجية قوية لتعقب الإرهابيين بأسلوب يحدث تغييرا، لكن مايكل هايدن كان يعيق التقدم ويحجب البيانات لأسباب تسلطية ضيقة الأفق.

بطبيعة الحال، كان لهايدن اتصالاته الخاصة، وبدأ يسمع تقارير بشأن مكائد جنرال الجيش الميداني (القوات البرية) ذي النجمتين هذا. حتى إن أحد مصادره أخبره بأن ألكسندر كان يطرق الأبواب في وزارة العدل، ويسأل عن السبيل إلى «محكمة مراقبة الاستخبارات الأجنبية»، التي كانت تمنح تفويضات باعتراض العملاء المشتبه فيهم، والجواسيس داخل حدود الولايات المتحدة. كانت هذه هي منطقة وكالة الأمن القومي، ولم يكن لدى أي أحد آخر أي شأن - قانوني أو سياسي أو غير ذلك - لأن يتحرى عنها أو يحوم حولها.

بدأ هايدن يشير إلى ألكسندر على أنه «حفيف نايكي» the Nike swoosh، على غرار رمز العلامة التجارية للأحذية الرياضية (خط مقوس يتلاشى)، والذي كان يحمل شعار «افعلها فقط» Just do it، وكان هايدن يرى أن هذا هو مختصر ملائم للطريقة التي كان ألكسندر يعمل بها.

لكن ألكسندر حاز ثقة رامسفيلد[6]، الذي لم يكن يروقه هايدن كثيرا، وكان يستحسن ذريعة أن وكالة الأمن القومي كانت بطيئة جدا. من خلال مراقبته التلميحات والقرائن، توقع هايدن ما سيحدث. وفي يونيو من العام 2001 وضع ترتيبا لتشارك قواعد بيانات معينة مع «فورت بيلفوار». استمر انعدام الثقة المتبادل، إذ كان ألكسندر يرتاب في أن هايدن لم يكن يعطيه كل البيانات الجيدة، وكان هايدن يرتاب في أن ألكسندر لم يكن ينزع بيانات معلومات الأمريكيين الشخصية - الذين لم يكن هناك مفر من أن تتصيدهم المراقبة - كما يقتضي القانون(*).

(*) من المفارقات التي تدعو إلى السخرية أنه بينما كان هايدن يشكو[7] من أن ألكسندر ربما لا يتعامل مع بيانات وكالة الأمن القومي بأسلوب قانوني صارم، فإن هايدن كان ينفذ برنامج مراقبة محليا مريبا من الناحية القانونية، للتنقيب في قاعدة البيانات ذاتها التي لدى وكالة الأمن القومي، بما في ذلك المحادثات الهاتفية والنشاط على الإنترنت لمواطنين أمريكيين. برر هايدن هذا البرنامج، الذي أطلق عليه اسم رمزي هو ستيلار ويند «الرياح النجمية» (Stellar Wind)، على اعتبار أنه كان صحيحا؛ لأن الرئيس بوش كان هو الذي أمر به، واعتبره محامو وزارة العدل مشروعا.

في نهاية المطاف، فإن الأدوات التحليلية التي كان قد أثنى عليها ألكسندر وهيث كثيرا لم تظهر زوايا جديدة، ولم تكشف عن أي إرهابيين. فشل هايدن وألكسندر في الكشف عن علامات لهجمات 11 سبتمبر.

وبعد أربعة أعوام من الحادي عشر من سبتمبر، وعقب فترة وجيزة - بوصفه الضابط الأعلى لاستخبارات الجيش الميداني في البنتاغون - استولى ألكسندر على القصر في «فورت ميد»، مستحوذا على قواعد البيانات، وأحضر معه هيث مستشارا علميا له.

خلال الأشهر الأولى من توليه المنصب، لم يكن لدى ألكسندر وقت للمضي قدما في أجندته الخاصة بالبيانات الواصفة. كانت الحرب في العراق على رأس الأولويات؛ إذ كانت تعني له تخفيف القيود التقليدية عن موجودات وكالة الأمن القومي، ووضع فرق استخبارات الإشارة (سيجينت) في اتصال دائم بالقادة على الأرض، وتكليف صفوة مخترقي الحاسوب في «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو) بمهمة التعامل مع الاحتياجات المحددة والمصممة وفقا لمتطلبات القوات الخاصة التابعة للجنرال ماكريستال في قتالهم ضد المتمردين.

كان يجب على ألكسندر أيضا إصلاح بعض العطب داخل وكالة الأمن القومي.

قبل أسبوع من وصول ألكسندر إلى «فورت ميد»، أوقف ويليام بلاك William Black، نائب هايدن طوال الأعوام الخمسة السابقة، مشروع «تريلبليزر» (الرائد) Trailblazer، وهو المشروع العملاق الذي كانت الوكالة تقوم به من خلال التعهيد، لرصد واعتراض وتمحيص (غربلة) الاتصالات من الشبكة العالمية الرقمية.

كان مشروع «تريلبليزر» قد استنفد 1.2 مليار دولار[8] من موازنة الوكالة منذ بداية العقد، وكان قد ثبت أنه كارثة؛ إذ إنه كان منبعا لسوء إدارة المؤسسة، وتجاوزات في التكاليف، وكما رآه ألكسندر بصورة أدق، كان خطأ مفاهيميا فادحا. لقد كان نظاما أحاديا جامدا (monolithic system) مترابطا ومتداخلا في قطعة واحدة، جرى بناؤه مرتكزا على حواسيب ضخمة لالتقاط ومعالجة طوفان البيانات الرقمية. كانت المشكلة هي أن التصميم كان بسيطا جدا. كانت القوة الحسابية المفرطة تحقق نجاحا في حقبة استخبارات الإشارات التماثلية (التناظرية)، حينما كانت المحادثة برمتها، أو إرسال الفاكس، ينساب عبر السلك ذاته، أو عبر دفقة

راديوية (لاسلكية). لكن البيانات الرقمية كانت تتدفق عبر الفضاء السيبراني في حزم، تنفصل إلى شذرات صغيرة جدا، كل شذرة كانت تسلك أسرع طريق ممكن قبل إعادة التجميع عند الوجهة المقصودة. لم يعد يكفي جمع الإشارات من المستشعرات (أجهزة الاستشعار) في الميدان، ثم بعد ذلك معالجة البيانات في المقر؛ إذ كانت هناك إشارات كثيرة جدا، تتسابق بسرعة كبيرة عبر العديد من المخدمات والشبكات. لم يكن ممكنا «توسيع نطاق» مشروع «تريلبليزر» Trailblazer إلا إلى حد معين فقط، قبل أن تغمره بحار من البيانات. كان ينبغي أن تقوم المستشعرات بمعالجة المعلومات، ودمجها مع التغذية من المستشعرات الأخرى، آنيا في الوقت الحقيقي.

من ثم، كانت مهمة ألكسندر الأولى هي الاستعاضة عن «تريلبليزر»؛ بعبارة أخرى، استحداث منهج جديد كلية لاستخبارات الإشارة يناسب العصر الرقمي. كان أسلافه في العقد الماضي قد واجهوا التحدي ذاته، وإن كان على نحو أقل إلحاحا. كان كين مينهيان يمتلك الرؤية، لكنه كان يفتقر إلى المهارات الإدارية، وكان لدى مايك هايدن الفطنة والحنكة الإدارية، لكنه انصاع للدراية التقنية المفترضة في المقاولين (المتعهدين) الخارجيين، الذين قادوه إلى المجهول عبر طريق مكلف. كان ألكسندر هو أول مدير لوكالة الأمن القومي يدرك أن التكنولوجيا هي مركز المؤسسة، وكان يمكنه التحدث مع رجال عمليات استخبارات الإشارة، ومخترقي الحاسوب في «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو)، ومحللي «ضمان المعلومات» على مستواهم نفسه. كان ألكسندر في القلب منهم، واحدا منهم، إذ إنه كان عاشقا للحاسوب ومهووسا به أكثر منه سياسيا مخضرما. كان يقضي ساعات منبطحا على الأرض مع رفاقه المهرة العاشقين للحاسوب، يناقش المشكلات، والنهج والحلول الممكنة، إلى حد أن كبار مساعديه نصبوا مزيدا من الحواسيب في مكتبه في الطابق الثامن من البناية، لكي يستطيع العمل على الألغاز التقنية المحببة إليه، من دون قضاء كثير من الوقت بعيدا عن جداول الأعمال والقضايا الأوسع نطاقا التي كان لزاما عليه التصدي لها ومعالجتها باعتباره مديرا.

كان لدى ألكسندر قدرات تقنية ومقدرة على التحدث مع التقنيين بلغة مشتركة. نتيجة لذلك، وفي غضون أشهر، ابتكر هو وفريقه الخطوط المفاهيمية العريضة

لنظام جديد؛ وفي غضون عام، أطلقوا المراحل الأولى من برنامج جديد أطلقوا عليه اسم «تيربلانس» (صخب) Turbulence.

بدلا من نظام مفرد، «نظام أحادي جامد» مترابط ومتداخل في قطعة واحدة، يحاول تنفيذ كل شيء، كان «تيربلانس» يتألف من تسعة نظم أصغر[9]. من جهة، كانت النظم المختلفة بمنزلة دعم احتياطي أو نهج بديل، في حالة إخفاق الأنظمة الأخرى، أو حدوث تحول تكنولوجي كبير. على نحو أكثر تحديدا، كان كل من تلك النظم يقسم الشبكة إلى شرائح من نواح مختلفة. كانت بعض الأجزاء تعترض الإشارات من الأقمار الاصطناعية، والموجات الميكروويية، وكابلات الاتصالات؛ وأجزاء أخرى كانت تلاحق الهواتف الجوالة؛ والبعض الآخر كان يتنصت على شبكة الإنترنت ليلاحق حركة البيانات عبرها على مستوى حزم البيانات، اللبنة الأساسية للإنترنت ذاتها، وكانت إما تتعقب الحزم من منبعها، وإما ترقد على خط الاتصالات الرئيسي لحركة البيانات على الإنترنت (عادة بالتعاون مع كبار مزودي خدمات الإنترنت)، للكشف عن حزمة مستهدفة، ثم تنبيه مخترقي الحاسوب في «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو) لتولي المسؤولية.

لم تكن حنكة ألكسندر التقنية فقط هي التي جعلت برنامج «تيربلانس» ممكنا، بل كان أيضا ما قد حدث في الأعوام القليلة السابقة، من تقدم هائل في معالجة البيانات وتخزينها وفهرستها. تولى ألكسندر القيادة في «فورت ميد» تماما في اللحظة ذاتها التي تقاربت فيها رغباته مع الواقع في عالم الحواسيب.

على مدى العقد الذي أعقب ذلك، بينما كان برنامج «تيربلانس» يصل إلى مرحلة النضج، ويتفرع إلى برامج متخصصة (أطلق عليها أسماء، مثل: «تربين» Turbine، و«ترمويل» Turmoil، و«كوانتم ثيوري» (نظرية الكم) QuantumTheory، و«كوانتم إنسيرت» QuantumInsert، و«إكس كي سكور» XKeyscore)، كان برنامج «تيربلانس» يتبلور ويتطور إلى نظام عالمي شامل ومترابط تماما بعضه مع بعض، مما كان سيجعل الأجيال السابقة من استخبارات الإشارات تبدو عتيقة وغير متقنة الصنع مقارنة بها.

كان برنامج «تيربلانس» يعتمد على قواعد البيانات الضخمة ذاتها التي كان يستند إليها برنامج «تريلبليزر». كان الاختلاف هو أسلوب معالجة وغربلة البيانات

الذي كان - إلى حد بعيد - أكثر دقة، ومصمما خصيصا ليكون أكثر ملاءمة للبحث عن معلومات نوعية محددة، ومقولبا بإحكام أكثر وفقا للمسارات الفعلية للاتصالات الرقمية الحديثة من حزم وتدفقات. ولأن الاعتراضات كانت تتم في داخل الشبكة، فإنه كان من الممكن تتبع الهدف على الفور، آنيا في الوقت الحقيقي.

في المراحل الأولى من برنامج «تيربلانس»، انطلق برنامج مواز له، مشتق من المفاهيم التقنية ذاتها، متضمنا بعض أفراد من الفريق التقني ذاته، لكن تركيزه كان منصبا على منطقة جغرافية محددة. كان البرنامج يدعى «بوابة الوقت الحقيقي الإقليمية» (آر تي آر جي) Real Time Regional Gateway (RTRG)، وكانت مهمته الأولى هي مطاردة المتمردين في العراق.

بدأت «بوابة الوقت الحقيقي الإقليمية» (آر تي آر جي)[10] في أوائل العام 2007، تقريبا في الوقت نفسه الذي تولى فيه الجنرال ديفيد بترايوس David Petraeus قيادة قوات الولايات المتحدة في العراق، وإصدار الرئيس بوش أمرا ينص على «زيادة مفاجئة» في عدد تلك القوات. لقد كان بترايوس وألكسندر على وفاق أكثر من ثلاثين عاما، لقد كانا زميلي دراسة في «ويست بوينت»، منبع العلاقات الوطيدة والترابط بين ضباط الجيش الميداني، وكانا قد جددا علاقاتهما بعد ذلك بأعوام، باعتبارهما من قادة الألوية في «فورت براغ». حينما التقيا معا مجددا، حينما كان بترايوس يقود القتال في بغداد، كونا بطبيعتهما فريقا؛ إذ كان بترايوس يرغب في أن يكسب الحرب من خلال تنشيط تقنيات مكافحة التمرد، وكان ألكسندر حريصا على أن يجرف موارد وكالة الأمن القومي لمساعدته.

كان أكبر تهديد للجنود الأمريكيين في العراق هو العبوات الناسفة التي تُغرَس على جوانب الطرق. كان فيض المعلومات الاستخباراتية، بشأن مفجري القنابل ومواقعهم، ينهمر على حواسيب وكالة الأمن القومي، من اعتراضات الهواتف الجوالة، والصور التي تلتقطها طائرات الاستطلاع المسيرة من دون طيار، والأقمار الاصطناعية، وعدد وافر لا حصر له من المصادر الأخرى. لكن الأمر كان يستغرق ست عشرة ساعة حتى تصل البيانات إلى البنتاغون، ثم إلى «فورت ميد»، ثم إلى الفرق التقنية لإجراء التحليل، ثم العودة إلى مراكز الاستخبارات في بغداد، ثم إلى الجنود في الميدان؛ وكان ذلك وقتا طويلا جدا، إذ إن المتمردين حينئذ يكونون قد انتقلوا بالفعل إلى مكان آخر.

اقترح ألكسندر الاستغناء عن الوسطاء ووضع أجهزة ومحللي وكالة الأمن القومي داخل العراق. وافق بترايوس. بداية، أسسا مكانا لمشغل يكون بمنزلة وكالة أمن قومي مصغرة، في حظيرة طائرات أسمنتية تحت حراسة مشددة في قاعدة «بلد» الجوية في شمال بغداد. بعد فترة وجيزة كان بعض المحللين يخرجون في دوريات مع القوات المقاتلة، ويجمعون البيانات ويعالجونها في أثناء تحركهم. على مدار الأعوام القليلة التي تلت ذلك، جرى نشر ستة آلاف مسؤول من وكالة الأمن القومي في العراق، ولاحقا في أفغانستان؛ قتل منهم اثنان وعشرون، معظمهم بفعل العبوات الناسفة التي كانت تغرس على جانبي الطريق، حينما يكونون هم في الخارج مع القوات.

لكن جهودهم كان لها تأثير؛ ففي الأشهر القليلة الأولى، تقلصت الفترة الزمنية الفاصلة بين جمع المعلومات الاستخباراتية والعمل عليها من ست عشرة ساعة إلى دقيقة واحدة.

بحلول شهر أبريل، كانت القوات الخاصة تستخدم هذا الكنز من المعلومات الاستخباراتية؛ ليس فقط لاصطياد المتمردين، لكن أيضا للتحفظ على حواسيبهم المختزن داخلها رسائل بريد إلكتروني، وأرقام هواتف، وأسماء مستخدمين، وكلمات مرور تخص متمردين آخرين، بمن في ذلك قادة تنظيم القاعدة، المادة الأساس لصلب أحلام عظماء التجسس الجدد.

أخيرا، أصبح لدى ألكسندر وماكريستال مقومات الحملة السيبرانية الهجومية التي كانا قد ناقشاها مع جون أبي زيد، قبل ذلك بأربعة أعوام. كانت فرق وكالة الأمن القومي في قاعدة «بلد» الجوية تحمل كامل حاشيتها من خدع ومهارات تجسس. كانوا يعترضون رسائل البريد الإلكتروني الخاصة بالمتمردين؛ في بعض الحالات كانوا لا يرصدون سوى الرسائل المتبادلة لاكتساب معلومات استخباراتية جديدة؛ في حالات أخرى كانوا يحقنون برمجيات خبيثة لإيقاف تشغيل مخدمات المتمردين؛ وفي حالات أخرى كثيرة كانوا يرسلون إلى المتمردين رسائل بريد إلكتروني وهمية مصطنعة، يأمرونهم فيها بالالتقاء في وقت معين، في مكان محدد، حيث تكون القوات الخاصة الأمريكية مختبئة في انتظارهم لقتلهم والقضاء عليهم.

في العام 2007 وحده، فإن تلك النوعيات من العمليات[11]، التي تحققت بفضل مساعدة وكالة الأمن القومي، أدت إلى قتل نحو أربعة آلاف من المتمردين العراقيين.

لم يكن التأثير حاسما ساحقا[12]، ولم يقصد منه أن يكون كذلك، كانت الفكرة هي إعطاء فرصة لالتقاط الأنفاس، منطقة أمن، للفصائل السياسية في العراق لتسوية خلافاتهم، وتكوين دولة موحدة من دون قلق بشأن العبوات الناسفة التي تنفجر كل يوم. كانت المشكلة هي أن الفصيل الحاكم، لم يرغب في تسوية خلافاته مع الفصائل المتناحرة في الأوساط الأخرى... وهكذا، بعد مغادرة القوات الأمريكية، تجدد القتال الطائفي.

لكن العام 2007 كان عاما محوريا، شهد إخمادا هائلا للعنف؛ وترويض معظم المليشيات النشطة، أو استسلامها، أو استقطابها. كانت استراتيجية بترايوس لمكافحة التمرد لها علاقة بهذا الأمر، مثلما كان للأمر الذي أصدره بوش بخصوص «الزيادة المفاجئة» في عدد الجنود. لكن الفوز بالمكاسب التكتيكية لم يكن ممكنا من دون «بوابة الوقت الحقيقي الإقليمية» (آر تي آر جي) لوكالة الأمن القومي.

لم تكن «بوابة الوقت الحقيقي الإقليمية» هي الابتكار الوحيد الذي شهده العام في وسائل الحرب السيبرانية الهجومية.

في 6 سبتمبر[13]، بعد منتصف الليل مباشرة، حلقت أربع طائرات مقاتلة إسرائيلية من طراز إف - 15 في شرقي سورية، فوق مفاعل نووي كان يجري بناؤه بمساعدة علماء من كوريا الشمالية، وهدمته بوابل من القنابل والقذائف الموجهة بالليزر. صعق الرئيس السوري بشار الأسد لدرجة أنه لم يصدر أي احتجاج علني، فالتظاهر بأنه لم يحدث أي شيء أفضل من الاعتراف بمثل هذه الغارة الناجحة. الإسرائيليون أيضا لم يذكروا شيئا.

كان الأسد حائرا. في فبراير السابق، كان جنرالاته قد نصبوا بطاريات دفاع جوي روسية جديدة، وكانت الطواقم تتدرب عليها منذ ذلك الحين، وبسبب التوترات في هضبة الجولان، كانت الطواقم في الخدمة في ليلة الهجوم؛ غير أنهم لم يبلغوا عن أي طائرات ظهرت على شاشات الرادار الخاصة بهم.

تمكن الإسرائيليون من تنفيذ الهجوم الذي أطلق عليه الاسم الرمزي «عملية البستان» Operation Orchard؛ لأنه - قبل الموعد المحدد - كانت الوحدة 8200، وهي مكتبهم السري لوسائل الحرب السيبرانية، قد اخترقت نظام رادار الدفاع الجوي السوري. قامت الوحدة 8200 بذلك الاختراق باستخدام برنامج حاسوبي

يسمى «سوتر» Suter[14]، طوره مكتب سري تابع لسلاح الجو الأمريكي يدعى «بيغ سفاري» Big Safari. لم يعطل «سوتر» الرادار، وبدلا من ذلك عرقل وصلة البيانات التي تربط الرادار بشاشات مشغلي الرادار. في الوقت ذاته، اخترق «سوتر» إشارة الفيديو الخاصة بالشاشات، بحيث كان طاقم الوحدة 8200 يستطيع رؤية ما يشاهده مشغلو الرادار. إذا سار كل شيء على ما يرام، فإنهم كانوا سيشاهدون شاشات خالية من الأهداف، وسارت الأمور كلها على ما يرام.

هذا الأمر يعود بنا إلى الحملة التي شُنت في البلقان، قبل ذلك بعشرة أعوام، حينما خدعت الوحدة «جي - 39» بالبنتاغون، ووكالة الأمن القومي، ومركز عمليات المعلومات في وكالة الاستخبارات المركزية قيادة الدفاع الجوي الصربي، عن طريق الدخول في خطوط الاتصالات الخاصة بها، وأرسلت بيانات خاطئة كاذبة إلى شاشات الرادار الخاصة بها. وكانت الحملة الصربية لها جذورها التي تعود إلى قبل ذلك بخمسة أعوام، في الخطة التي حلم بتحقيقها محترفو استخدام برمجية «عفريت الاتصال الهاتفي» العاملون مع كين مينهيان في مركز سلاح الجو لوسائل الحرب السيبرانية في سان أنطونيو، لتحقيق مفاجأة جوية في غزو هايتي (الذي أُوقِف في نهاية الأمر) عن طريق التشويش على كل هواتف الجزيرة.

كانت الحملة الصربية وحملة هايتي حالتين كلاسيكيتين تقليديتين لوسائل حرب المعلومات في العصر ما قبل الرقمي، حينما كانت القوات المسلحة لكثير من الدول تدير اتصالاتها عبر خطوط الهاتف التجارية العمومية. استغلت «عملية البستان» تنامي الاعتماد على شبكات الحاسب، مثلما فعلت عملية وكالة الأمن القومي - قيادة العمليات الخاصة المشتركة في العراق - كانت هايتي والبلقان هما تجارب لوسائل الحرب السيبرانية الأولية (البدئية)، أما «عملية البستان» ومطاردة الجهاديين في العراق فإنهما وسمتا البداية الحقيقية.

قبل ذلك بأربعة أشهر ونصف الشهر[15]، في 27 أبريل 2007، اندلعت أعمال شغب في مدينة تالين Tallinn، عاصمة إستونيا Estonia، أصغر الجمهوريات السوفييتية الثلاث المطلة على بحر البلطيق، وأكثرها ميلا إلى الغرب، وتقع جنوب فنلندا مباشرة. كان شعب إستونيا قد استاء من حكم موسكو الذي دام منذ بداية الحرب العالمية الثانية، حينما بدأ الاحتلال. حينما سيطر ميخائيل غورباتشوف

Mikhail Gorbachev على الكرملين، وخفف من قبضته التي دامت نحو نصف قرن، قاد شعب إستونيا التمرد من أجل الاستقلال الذي ساد المنطقة، مما ساعد على انهيار الاتحاد السوفييتي. حينما اعتلى فلاديمير بوتين Vladimir Putin السلطة في مطلع القرن الحادي والعشرين، إثر موجة من الاستياء والحنين إلى أيام القوة العظمى، ازدادت حدة التوترات مجددا.

بدأت أعمال الشغب حينما رفض رئيس إستونيا، تحت ضغط من، قانونا كان سيزيل كل النصب التذكارية التي ظهرت خلال أعوام الاحتلال السوفييتي، بما في ذلك تمثال برونزي ضخم لأحد جنود الجيش الأحمر. خرج الآلاف من شعب إستونيا إلى الشوارع احتجاجا، منقضين على التمثال البرونزي في محاولة لإسقاطه بأنفسهم، لم يواجه كل هذا إلا بالأقلية الإثنية الروسية في البلدة الذين هبوا لصد الهجوم، معتبرين أن الاحتجاج هو إهانة للتضحيات التي قدمها الوطن الأم في زمن الحرب. تدخلت الشرطة ونقلت التمثال إلى مكان آخر، لكن المعارك في الشوارع استمرت، وعند تلك المرحلة تدخل بوتين، ليس بالقوات العسكرية، كما كان أسلافه ربما قد يفعلون، ولكن بهجمة من آحاد وأصفار.

كان مواطنو إستونيا البالغ تعدادهم 1.3 مليون مواطن، هم من بين الأكثر تقدما من الناحية الرقمية على كوكب الأرض؛ إذ إن نسبة كبيرة منهم كانوا موصولين بالإنترنت، وكانوا يعتمدون على خدمات النطاق الترددي العريض أكثر من سكان أي بلد آخر. في اليوم التالي لاضطرابات ليلة البرونز - كما كان يطلق عليها - تعرض مواطنو إستونيا لهجوم سيبراني عات، جرى غمر شبكاتهم ومخدماتهم بفيض غزير من البيانات، مما أدى إلى إيقاف تشغيلها. وبخلاف معظم هجمات حجب الخدمة التي كانت تميل إلى أن تسبب بعض الضرر مرة واحدة وغير متكررة، كان هذا الهجوم مستمرا ومتتابعا في ثلاث موجات منفصلة، مصحوبا بإصابات من برمجيات خبيثة ضارة تنتشر من حاسوب إلى آخر، عبر الأمة الصغيرة، في كل مناحي الحياة. طوال ثلاثة أسابيع، وبشكل متقطع طوال شهر كامل، لم يتمكن العديد من مواطني إستونيا من استخدام حواسيبهم فقط، ولكن هواتفهم، وحساباتهم البنكية، وبطاقات الائتمان، إذ إن كل شيء كان مرتبطا بشبكة أو بأخرى - البرلمان، ووزارات الحكومة، ووسائل الإعلام، والمتاجر، والسجلات العامة، والاتصالات العسكرية - كان كل ذلك ينهار.

طلبت إستونيا المساعدة بصفتها عضوا في حلف شمال الأطلسي (ناتو)، بموجب المادة الخامسة من معاهدة شمال الأطلسي التي تلزم الدول الأعضاء بالتعامل مع الاعتداء على إحداها على أنه اعتداء على الجميع. لكن الحلفاء كانوا متشككين. هل كان هذا اعتداء بهذا المعنى؟ هل كان عملا من أعمال الحرب؟ بقي السؤال مفتوحا من دون إجابة، ولم يَجرِ إرسال أي قوات.

غير أن خبراء الحاسوب في الغرب هبوا - بمبادرة منهم - للدفاع عن إستونيا؛ إذ انضموا إلى الحركة الكبيرة لقراصنة الحاسوب الأخلاقيين المهرة (ذوي القبعات البيضاء) داخل إستونيا وساعدوهم. استخدموا مجموعة متنوعة من التقنيات العريقة، وتتبعوا العديد من المتسللين وطردوهم؛ مما خفف من الآثار التي كانت ستنشب لو أن حكومة تالين كانت هي المورد الوحيد للمقاومة والدفاع.

نفى مسؤولو الكرملين ضلوعهم في الهجوم، ولم يستطع الغربيون العثور على أدلة قاطعة تشير إلى وجود متهم واحد. ومن بين أسباب كثيرة، كان أحدها هو إحجامهم عن اعتبار الهجمات السيبرانية سببا للاحتجاج وإنفاذ المادة الخامسة. كان تحديد مصدر الهجوم السيبراني مسألة صعبة بطبيعتها، وأيا كان من ابتدأ هذا الهجوم، فإنه كان قد غطى آثار مساراته بيد خبيرة وأسلوب ينم عن احترافية وإتقان. مع ذلك، تعقب خبراء التحليل الجنائي التعليمات البرمجية (الكود) للبرمجيات الخبيثة، وأرجعوها إلى لوحة مفاتيح سيريلية(*). ردا على ذلك، ألقت سلطات الكرملين القبض على عضو واحد من «منظمة الشباب القوميين» (ناشي) nationalist youth organization (Nashi)، وهي الكلمة الروسية لـ «ملكنا» (خاصتنا) Ours، وألزمته بدفع غرامة تعادل ألف دولار، وأعلنت أن الجريمة قد جرى حلها. لكن لم يصدق أحد أن مواطنا متواضعا بمفرده، أو مجموعة خاصة صغيرة، كان يمكن أن تجد، فضلا عن كونها تخترق، بعض مواقع الإنترنت الإستونية الحيوية التي كان قد جرى تعطيلها جميعا دفعة واحدة في الوقت نفسه، ولمثل هذه الفترة الطويلة.

اتضح أن الضربات السيبرانية في إستونيا كانت بمنزلة تدريب نهائي (بروفة نهائية) لحملة عسكرية منسقة، فبعد مرور ما يزيد قليلا على العام، أطلقت

(*) هي الأبجدية التي أبتكرتها الإمبراطورية البلغارية في القرون الوسطى. [المحرر].

روسيا عمليات جوية، وبرية، وبحرية، وسيبرانية متزامنة ضد جورجيا، الجمهورية السوفييتية السابقة.

منذ نهاية الحرب الباردة، سادت توترات بين موسكو وحكومة جورجيا المستقلة حديثا بشأن أوبلاستات[*] (مقاطعات) أوسيتيا الجنوبية South Ossetia وأبخازيا Abkhazia الصغيرتين، هي رسميا جزء من جورجيا، ولكنها تكتظ بسكان من أصل روسي. في 1 أغسطس 2008، قصف الانفصاليون في أوسيتيا[16] قرية تسخينفالي Tskhinvali الجورجية. في ليلتي السابع والثامن من شهر أغسطس، حُشِد جنود جورجيا، وقُمِع الانفصاليون، واستُعيدت البلدة في غضون ساعات قليلة. في اليوم التالي، تحت ذريعة «إنفاذ السلام»، دخلت القوات والدبابات الروسية إلى القرية، مدعومة بضربات جوية وحصار بحري على طول الساحل.

في اللحظة ذاتها التي عبرت فيها الدبابات والطائرات خط حدود أوسيتيا الجنوبية، جرى اختراق أربعة وخمسين موقع ويب خاصة بجورجيا - مواقع ويب ذات صلة بوسائل الإعلام، والشؤون المالية، والوزارات الحكومية، والشرطة، والقوات المسلحة - وأُعيد توجيهها، هي وكامل خدمة الإنترنت في الدولة، إلى مخدمات روسية، قامت بإغلاقها. لم يستطع مواطنو جورجيا الوصول إلى معلومات بشأن ما الذي كان يحدث؛ وواجه الضباط في جورجيا صعوبة في إرسال الأوامر إلى قواتهم؛ وواجه السياسيون في جورجيا فترات تأخير طويلة عند محاولتهم التواصل مع بقية العالم. نتيجة لذلك، كانت قنوات الدعاية الروسية هي أول من عرض على العالم نسخة موسكو من الأحداث. كانت حالة كلاسيكية نموذجية لما كان في يوم من الأيام يسمى وسائل حرب المعلومات، أو وسائل الحرب المضادة للقيادة والسيطرة؛ وهي حملة لإرباك، أو بلبلة، أو تضليل العدو؛ ومن ثم إضعاف، أو تأخير، أو تدمير قدرته على صد هجوم عسكري.

أيضا، سرق قراصنة الحاسوب من بعض مواقع الإنترنت مواد منحتهم معلومات استخباراتية ذات فائدة بشأن جيش جورجيا - عملياته، وتحركاته، والبيانات الصادرة عنه - مما كان يمكن القوات الروسية من التفوق عليهم بسرعة أكبر.

(*) «الأوبلاست»: هي كلمة روسية تعني «منطقة»، وهي تشير إلى محافظة أو مقاطعة من حيث التقسيم الإداري، وتعد من أكثر الكيانات شيوعا في روسيا الاتحادية. [المترجم].

كما هي الحال مع إستونيا، نفى المتحدثون باسم الكرملين إطلاق الهجمات السيبرانية، على الرغم من أن التوقيت الذي جرى تنسيقه بدقة بالغة مع الأشكال الأخرى للهجمات أشاع شكوكا بالغة بشأن ادعاءاتهم بالبراءة.

بعد أربعة أيام من القتال، انسحب جيش جورجيا. بعد مضي فترة وجيزة، أقر البرلمان الروسي رسميا أن أوسيتيا الجنوبية وأبخازيا هما ولايتان مستقلتان. اعترضت جورجيا على هذا الوضع، ومعها جزء كبير من بقية العالم، كانوا يرون الجيوب (الأماكن المحصورة) على أنها أراض جورجية محتلة، لكن لم يكن هناك الكثير مما يمكنهم فعله حيال ذلك.

في أثناء الستة عشر شهرا ما بين أبريل من العام 2007 وحتى أغسطس من العام 2008، حينما اخترقت أمريكا البريد الإلكتروني للمتمردين العراقيين، وخدعت إسرائيل الدفاعات الجوية السورية، وغمرت روسيا مخدمات إستونيا وجورجيا، شهد العالم بزوغ فجر حقبة جديدة في وسائل الحرب السيبرانية - استيفاء لإنجاز عشر سنوات من الدراسات، وتجارب نماذج المحاكاة، واختبار أولي في صربيا في بداية العقد.

كانت عملية إستونيا هي طعن في الإكراه والقسر السياسي، وعلى الرغم من أنها فشلت في هذا السياق، إذ إنه في النهاية نُقِل تمثال جندي الجيش الأحمر من وسط مدينة تالين إلى مقابر عسكرية على مشارف المدينة.

كانت العمليات الثلاث الأخرى ناجحة، لكن دور السيبرانية في كل منها كان تكتيكيا، وعاملا مساعدا للعمليات العسكرية التقليدية، تماما مثلما كان دور الرادار، وتكنولوجيا التخفي، والتدابير الإلكترونية المضادة في صراعات سابقة. كذلك، ربما لم تكن آثارها لتدوم طويلا إذا كانت الصراعات استمرت فترة أطول، كان من المرجح أن الدول المستهدفة ستجد أساليب لإبعاد، أو تشتيت، أو تعطيل الهجمات السيبرانية، تماما مثلما فعل شعب إستونيا بمساعدة حلفاء الغرب. حتى في الحرب التي استمرت أربعة أيام في أوسيتيا الجنوبية، تمكنت جورجيا من إعادة توجيه بعض مخدماتها إلى دول غربية، وتصفية بعض التسللات الروسية. تطور الهجوم السيبراني إلى حرب سيبرانية ذات اتجاهين، مع تكتيكات ومناورات مرتجلة.

كانت وسائل حرب المعلومات في كل تجسيداتها، على مر القرون، مثل المقامرة، وكان المردود منها يستمر فترة وجيزة؛ وفي أفضل الأحوال فترة لا تكفي إلا لأن يعبر

الجواسيس، أو القوات، أو السفن، أو الطائرات أحد الحدود من دون أن يجري كشفها، أو لإعاقة واعتراض رسالة حاسمة، أو إرسالها واستقبالها.

أحد الأسئلة التي بقيت بشأن هذا الفصل الأخير في عصر الإنترنت، كان عما إذا كانت الآحاد والأصفار التي تئز عبر الفضاء الإلكتروني قادمة من الجانب الآخر من العالم، تستطيع أن تلحق ضررا ماديا بأصول دولة ما. كانت الفقرات الأكثر مدعاة للقلق في تقرير «مارش»، وعدة دراسات أخرى، قد أشارت إلى قابلية تأثر وعدم تحصن شبكات الطاقة الكهربائية، وخطوط أنابيب النفط والغاز، والسدود، والسكك الحديد، ومحطات المياه، وغيرها من أجزاء البنية الأساسية الحيوية بالغة الأهمية في الدولة، التي جميعها يتزايد التحكم فيها من خلال حواسيب تعمل باستخدام أنظمة تجارية. حذرت الدراسات من أن عملاء الاستخبارات الأجنبية، أو عصابات الجريمة المنظمة، أو الأناركيين (مثيري الفوضى) الشريرين كان في إمكانهم إيقاف تشغيل هذه الأنظمة وإسقاطها بالهجمات السيبرانية من أي مكان على كوكب الأرض. بعض التدريبات المصنفة على أنها سرية، بما في ذلك مرحلة المحاكاة لمناورة تدريب «المتلقي المؤهل»، افترضت وجود مثل هذه الهجمات. لكن هل كانت السيناريوهات معقولة ومقبولة؟ هل كان يمكن حقيقة لقرصان حاسوب ماهر أن يدمر شيئا ماديا؟

للإجابة عن ذلك السؤال، أجرت وزارة الطاقة في 4 مارس 2007 تجربة أُطلق عليها اسم «اختبار المولد الكهربائي أورورا» Aurora Generator Test[17].

أدار الاختبار ضابط استخبارات بحري متقاعد يدعى مايكل أسانتي Michael Assante. بعد هجمات 11 سبتمبر بفترة وجيزة، كُلِّف أسانتي بمركز حماية البنية الأساسية التابع لمكتب التحقيقات الفدرالي الذي كان قد أُنشئ في أعقاب هجوم «الشروق الشمسي»، وعملية «متاهة ضوء القمر»، أول الاختراقات السيبرانية الكبيرة للشبكات العسكرية الأمريكية. وبينما كان تركيز معظم محللي المركز منصبا على فيروسات الإنترنت، كان أسانتي يفحص قابلية تأثر أنظمة التحكم المؤللة التي تدير شبكات الطاقة الكهربائية، وخطوط الأنابيب، وغيرها من البنى الأساسية الحرجة التي كانت قد ورد تصنيفها في تقرير «مارش».

بعد ذلك ببضعة أعوام تقاعد أسانتي من سلاح البحرية، وذهب للعمل نائب رئيس وكبير مسؤولي الأمن في شركة الطاقة الكهربائية الأمريكية، التي كانت توصل

الكهرباء إلى ملايين العملاء في جميع أنحاء الجنوب، والغرب الأوسط، ووسط الأطلسي. أثار أسانتي تلك المسائل عدة مرات مع زملائه من التنفيذيين. ردا على ذلك، كان زملاؤه قد أقروا بأنه كان من الممكن أن يخترق أحد نظام التحكم ويتسبب في انقطاع التيار الكهربائي، لكنهم أضافوا أن الضرر سيكون قصير الأجل، إذ إن أحد التقنيين كان سيستبدل قاطع الدائرة، وستعود الأضواء. لكن أسانتي كان يهز رأسه. في السابق في مكتب التحقيقات الفدرالي، كان أسانتي قد تحدث مع مهندسي الحماية والمراقبة، صفوة المتخصصين، الذين ذكروه بأن قواطع الدوائر الكهربائية هي مثل المصاهر (الصمامات)، وظيفتها هي حماية المكونات باهظة التكلفة، مثل مولدات الطاقة، التي كان استبدالها أصعب بكثير، ويستغرق وقتا أطول. من المرجح أن مخترقا شريرا لم يكن ليتوقف عند تفجير قاطع الدائرة الكهربائية، إذ كان سيتمادى لإتلاف المولد أو تدميره.

أخيرا اقتنعوا بأن هذا ربما يمثل مشكلة، أوفده رؤساء أسانتي إلى «مختبر أيداهو القومي» Idaho National Laboratory، وهو مِرفق أبحاث فدرالي على مساحة 890 ميلا مربعا في صحراء البراري، خارج شلالات أيداهو، لدراسة القضايا بمزيد من التعمق. بداية، أجرى أسانتي تحليلات رياضية، ثم اختبارات منضدية لنماذج مصغرة، وأخيرا أعد تجربة واقعية. كانت وزارة الأمن الداخلي قد اضطلعت أخيرا بمشروع بشأن أخطار الفضاء السيبراني الأكثر إثارة للقلق، لذا وافق مديروها على المساعدة في تمويل التجربة.

كان الهدف من اختبار أورورا هو مولد طاقة كهربائية بقدرة 2.25 ميغاوات، يزن سبعة وعشرين طنا، مثبتا داخل إحدى غرف الفحص في المختبر. بإشارة من واشنطن، حيث كان المسؤولون يراقبون الاختبار على شاشة فيديو، لم يكتب أحد التقنيين سوى واحد وعشرين سطرا من التعليمات البرمجية الخبيثة إلى مُرحِّل رقمي digital relay جرى توصيله بالمولد. فتحت التعليمات البرمجية قاطع الدائرة في نظام حماية المولد، ثم أغلقته قبل أن يستجيب النظام، مما جعل عملياته خارج المزامنة. على نحو فوري تقريبا، اهتز المولد[18]، وطارت بعض أجزائه. بعد ذلك ببضع ثوان اهتز مجددا، ثم نفث دخانا أبيض وسحابة ضخمة من الدخان الأسود. كانت الماكينة ميتة.

قبل الاختبار، أدرك أسانتي وفريقه أنه ستكون هناك خسائر. هذا ما كانت تحليلاتهم وتجارب نماذج المحاكاة قد تنبأت به. لكنهم لم يتوقعوا حجم الخسائر أو السرعة التي كانت ستحدث بها. استغرق الاختبار ثلاث دقائق فقط، من البداية وحتى الانهيار، وكان سيستغرق دقيقة أو اثنتين أقل، بيد أن الطاقم كان يوقف التجربة مؤقتا لتقييم كل مرحلة من مراحل الضرر قبل الاستمرار.

إذا كانت الاشتباكات العسكرية في العام 2007 - في العراق، وسورية، والجمهوريات السوفييتية السابقة - قد أكدت أن الأسلحة السيبرانية يمكن أن تؤدي دورا تكتيكيا في وسائل حرب العصر الجديد، فقد كشف «اختبار المولد الكهربائي أورورا» أنها قد تؤدي دورا استراتيجيا أيضا، باعتبارها وسائل سيطرة أو أسلحة دمار شامل، لا تختلف في ذلك عن الأسلحة النووية. بطبيعة الحال، كانت الأسلحة السيبرانية ستسبب تدميرا أقل بكثير من القنابل الذرية أو الهيدروجينية، لكن الحصول عليها أيسر بكثير، إذ إنه ليست هناك ضرورة إلى «مشروع مانهاتن»(*)، الأمر لا يتطلب سوى شراء حواسيب وتدريب المخترقين، وستكون آثارها بسرعة البرق.

حدثت في الماضي دلائل عملية مماثلة لهذه التأثيرات، وإن كانت أقل حدة ومأساوية. في العام 2000 اخترق موظف ساخط وناقم[19] كان يعمل في أحد مراكز أستراليا لمعالجة المياه، حواسيبها المركزية، وأرسل أوامر عطلت المضخات، مما سمح لمياه المجارير (الصرف الصحي) الخام بأن تتدفق إلى الماء. في العام التالي اقتحم قراصنة الحاسوب مخدمات إحدى شركات كاليفورنيا التي كانت تنقل الطاقة الكهربائية في جميع أنحاء الولاية، ثم فحصوا شبكتها وتقصوها طوال فترة أسبوعين قبل الإيقاع بهم.

بعبارة أخرى، كان معروفا منذ زمن طويل أن المشكلة حقيقية وليست نظرية أو افتراضية فقط، لكن بضع شركات هي التي كانت قد اتخذت خطوات نحو الحل. لم تكن أي من الدوائر الحكومية قد أقدمت على ذلك؛ إذ إن أولئك الذين كان لديهم

(*) «مشروع مانهاتن»: كان مشروعا للبحث والتطوير في أثناء الحرب العالمية الثانية، أنتج أول أسلحة نووية. كان المشروع بقيادة الولايات المتحدة، وبدعم من المملكة المتحدة وكندا. بدأ المشروع متواضعا في العام 1939، لكنه نما لتوظيف أكثر من 130 ألف شخص، وكلف نحو ملياري دولار (نحو 22 مليار دولار أمريكي في العام 2016). كان أكثر من 90 في المائة من التكلفة لبناء المصانع وإنتاج المواد الانشطارية، وأقل من 10 في المائة لتطوير الأسلحة وإنتاجها. أجريت الأبحاث والإنتاج في أكثر من 30 موقعا عبر الولايات المتحدة والمملكة المتحدة وكندا. [المترجم].

المقدرة كانوا يفتقرون إلى السلطة القانونية، في حين كان أولئك الذين لديهم السلطة القانونية يفتقرون إلى المقدرة؛ ولأن الإجراء والتنفيذ كانا صعبين، لذا كان التهرب والمراوغة سهلين. لكن بالنسبة إلى كل من شاهد مقطع الفيديو الخاص باختبار المولد الكهربائي أورورا، لم يعد التهرب أو التملص خيارا.

إن أحد أكثر مشاهدي الفيديو اهتماما، وقد عرضه على المسؤولين في جميع أنحاء العاصمة، بدءا من الرئيس إلى من دونه، كان المدير السابق لوكالة الأمن القومي الذي صاغ وابتكر عبارة «وسائل حرب المعلومات»، الأدميرال مايك ماكونيل.

10

اليانكي(*) صائد الظباء

«كانت هناك مكاسب من الدخول إلى شبكات المتمردين، وعرقلة اتصالاتهم، وإرسال رسائل بريد إلكترونية مزيفة تحدد لهم وجهة يذهبون إليها، ثم إرسال وحدة عمليات خاصة لقتلهم حال وصولهم إلى هناك»

في 20 فبراير، قبل أسبوعين من «اختبار المولد الكهربائي أورورا»، أدى مايك ماكونيل اليمين الدستورية باعتباره مدير الاستخبارات القومية. كان هذا منصبا جديدا في واشنطن، استُحدث قبل ذلك بعامين فقط، في أعقاب تقرير لجنة الحادي عشر من سبتمبر الذي خلص إلى أن مؤامرة تنظيم القاعدة للاعتداء على مركز التجارة العالمي نجحت لأن أجهزة الاستخبارات المشتتة في البلاد - مكتب التحقيقات الفدرالي، ووكالة الاستخبارات المركزية، ووكالة الأمن القومي،

(*) مصطلح «يانكي» Yankee له عدة معان متداخلة، جميعها تشير إلى أشخاص من الولايات المتحدة. تعتمد الاستخدامات المختلفة على السياق، فخارج الولايات المتحدة يُستخدم على نحو غير رسمي للإشارة إلى أي أمريكي، بمن في ذلك الجنوبيون. داخل مناطق الجنوب الأمريكي، فهو مصطلح سائد يشير إلى جميع الشماليين، أو تحديدا إلى أولئك الذين أتوا من منطقة «نيو إنغلاند». وفي أثناء الحرب الأهلية الأمريكية، كان يطلقه الكونفدراليون على جنود الجيش الاتحادي. [المترجم].

وبقية الدوائر الأخرى - لم تكن تتواصل بعضها مع بعض، ومن ثم لم تكن تستطيع ربط جميع الأمور معا. كان منصب مدير الاستخبارات القومية منصبا وزاريا، ويحمل مسمى إضافيا هو المستشار الخاص للرئيس، كان من المزمع أن يكون بمنزلة مدير فوقي أعلى لينسق الأنشطة والنتائج بين كل أجهزة الاستخبارات، لكن كان يرى كثيرون المنصب على أنه مجرد مستوى إداري إضافي. حينما استُحدث المنصب[1]، عرضه الرئيس بوش على روبرت غيتس، الذي كان مديرا لوكالة الاستخبارات المركزية، ونائبا لمستشار الأمن القومي خلال فترة رئاسة جورج بوش الأب، لكن غيتس رفض المنصب حينما علم أنه لن تكون لديه سلطة إعداد الموازنات، أو تعيين الموظفين أو إقالتهم.

لم يكن لدى ماكونيل أي مشكلة فيما يتعلق بالقيود الإدارية للوظيفة، فقد قبلها بهدف واحد في ذهنه، هو وضع السيبرانية، لاسيما الأمن السيبراني، على جدول أعمال الرئيس.

في السابق، في أوائل التسعينيات من القرن العشرين وحتى منتصفها، وبوصفه مديرا لوكالة الأمن القومي، كان ماكونيل قد مر بالجولة الأفعوانية سريعة التقلبات نفسها، التي كان قد عاناها الكثير من الأشخاص الآخرين في «فورت ميد»، إذ إنه كان هناك اندفاع متحمس مذهل نحو الأعاجيب التي كانت فرق استخبارات الإشارة (سيجينت) التابعة للوكالة تستطيع أن تؤديها، يعقبه إدراك أنه مهما كان ما يمكننا فعله بأعدائنا، فإن أعداءنا كان يمكنهم أن يفعلوه بنا في وقت قريب وفي العقد الذي أعقب ذلك، تعمق الشعور بالرهبة نظرا إلى تزايد اعتماد أمريكا على شبكات الحاسوب الهشة وغير الحصينة.

بعد أن ترك ماكونيل وكالة الأمن القومي في أوائل العام 1996، جرى توظيفه بواسطة شركة بووز آلين، إحدى أقدم شركات الاستشارات الإدارية على طول ضاحية بيلتواي Beltway الضخمة في العاصمة، وحولها إلى مقاول (متعهد) ذي مركز قوة لدوائر استخبارات الولايات المتحدة - مركز بحث وتطوير استخبارات الإشارة وبرامج الأمن السيبراني، فضلا عن كونها ملاذا لتوظيف كبار موظفي وكالة الأمن القومي ووكالة الاستخبارات المركزية باعتبارهم ينتقلون جيئة وذهابا بين القطاعين العام والخاص.

مع قبوله وظيفة مدير الاستخبارات القومية، تخلى ماكونيل عن راتب يتكون من سبعة أرقام، لكنه كان يراها فرصة فريدة لتحويل أهوائه وخواطره السيبرانية

إلى سياسة. (إضافة إلى ذلك، فإن التضحية لم تصمد على المدى الطويل، إذ إنه بعد عودته إلى الحكومة وقضاء عامين، عاد ماكونيل إلى الشركة). سعيا إلى تحقيق هذا الهدف، بقي ماكونيل قريبا من المكتب البيضاوي بقدر ما كان يستطيع، عارضا الإحاطة الاستخبارية على الرئيس في بداية كل يوم. كان ماكونيل بارعا وذا دهاء في الأمور الإدارية، ويتكلم بتؤدة وتشدق على نحو عفوي يخفي حدته الليزرية، أيضا كان ماكونيل، في لحظات حاسمة، يدخل إلى المكتب على المساعدين والوزراء من ذوي العلاقة بسياسة الأمن السيبراني، سواء كانوا يدركون ذلك أو لا. لم يقتصر ذلك على الأشخاص المعنيين المعتادين من هيئة موظفي الخارجية، والدفاع، ومجلس الأمن القومي، ولكن أيضا وزارات الخزانة، والطاقة، والتجارة؛ لأن البنوك، والمرافق، والمؤسسات الأخرى، كانت على نحو خاص عرضةً للهجوم. لم يكن مفاجئا أن بضعة من هؤلاء المسؤولين كانوا في غفلة وغير مدركين للمشكلة، مما أثار استياء ماكونيل.

لذا، أخرج ماكونيل من جعبته حيلة متقنة. كان سيُحضِر إلى أمين مجلس الوزراء نسخة من مذكرة، وكان سيقول له وهو يسلمه إياها: ها هي، أنت كتبت هذه المذكرة الأسبوع الماضي، حصل الصينيون عليها بعد اختراقهم الحاسوب الخاص بك، ونحن استعدناها من الحاسوب الخاص بهم بعد اختراقه.

جذب هذا انتباههم، وفجأة، بدأ المسؤولون الذين لم يكن أحد منهم قد سمع مطلقا بشأن السيبرانية، بدأوا في إيلاء الموضوع اهتماما كبيرا، وطلب بعضهم أن يمدهم ماكونيل بإحاطة شاملة. رويدا رويدا، وعلى نحو هادئ، كان ماكونيل يبني دائرة مناصرين رفيعة المستوى لدعم خطة عمله.

في أواخر أبريل تلقى الرئيس بوش طلبا للتصريح بعمليات هجومية سيبرانية ضد المتمردين في العراق. كانت هذه هي الخطة التي شحذها وصقلها طوال أشهر الجنرالات أبي زيد، وبترايوس، وماكريستال، وألكسندر. أخيرا أُرسلت إلى قمة التسلسل القيادي من خلال وزير الدفاع الجديد، روبرت غيتس، الذي كان قد عاد إلى الحكومة قبل ماكونيل بشهرين فقط، ليحل محل دونالد رامسفيلد الذي أُطيح به.

من تجاربه وخبراته في وكالة الأمن القومي وشركة «بووز آلين»، كان ماكونيل يفهم طبيعة وأهمية هذا الاقتراح. كان جليا أن هناك مكاسب هائلة من الدخول إلى شبكات المتمردين، وعرقلة اتصالاتهم، وإرسال رسائل بريد إلكتروني مزيفة تحدد لهم

وجهة يذهبون إليها، ثم إرسال وحدة عمليات خاصة لقتلهم حينما يصلون إلى هناك. لكن، كانت هناك أخطار أيضا، إذ إن إدراج برمجيات خبيثة ضارة في البريد الإلكتروني للمتمردين ربما يؤدي إلى إصابة مخدمات أخرى في المنطقة، بما في ذلك مخدمات القوات المسلحة الأمريكية، والمدنيين العراقيين الذين لم تكن لهم علاقة بالنزاع. إنها كانت محاولة معقدة ومتشابكة، لذا رتب ماكونيل لقاء مع الرئيس لمدة ساعة لشرح أبعادها الكاملة.

على الرغم من ذلك، كان شيئا نادرا أن يُحاط رئيس بشأن العمليات الهجومية السيبرانية التي لم يكن هناك الكثير منها عند تلك المرحلة ووصل المقترح إلى لحظة حاسمة، بعد بضعة أشهر من طلب بوش زيادة مفاجئة في القوات والتحول إلى استراتيجية جديدة، وقائد جديد، ووزير دفاع جديد. لذا، فإن جلسة إحاطة ماكونيل[2]، التي انعقدت في 16 مايو، حضرها مجموعة كبيرة من المستشارين، هم: نائب الرئيس تشيني، ووزير الدفاع غيتس، ووزيرة الخارجية كوندوليزا رايس، ومستشار الأمن القومي ستيفن هادلي Stephen Hadley، ونائب رئيس الهيئة المشتركة لرؤساء الأركان الأدميرال إدموند جيامباستياني Edmund Giambastiani (كان رئيس الهيئة المشتركة لرؤساء الأركان، الجنرال بيتر بيس Peter Pace، مسافرا)، ووزير الخزانة هنري بولسون Henry Paulson، ومدير وكالة الأمن القومي الجنرال كيث ألكسندر، تحسبا لحالة ما إذا سأل أحدهم عن تفاصيل تقنية.

مثلما تبين، لم تكن هناك حاجة إلى المناقشة. التقط بوش الفكرة سريعا[3]، مستنتجا أن الجانب الإيجابي المشرق مغرٍ، ومساوئ الجانب السلبي ضئيلة وعديمة الأهمية. بعد عشر دقائق من بداية جلسة إحاطة ماكونيل التي كان من المفترض أن تستغرق ساعة، اختصر بوش الأمور وأقر الخطة.

ساد الهدوء الغرفة. ما الذي كان ماكونيل سيقوله الآن؟ هو لم يكن قد خطط لهذه الفرصة، لكنها بدت لحظة مثالية لضربته والترويج لما كان قد قَبِل الوظيفة من أجله، فأعد العدة وشحذ الهمة.

بدأ ماكونيل: سيدي الرئيس، نحن جئنا لنتحدث إليك بشأن الهجوم السيبراني لأننا نحتاج إلى تصريح منك للقيام بتلك العمليات، لكننا لم نتحدث إليك كثيرا بشأن الدفاع السيبراني.

نظر بوش إلى ماكونيل متسائلا، إذ إنه كان قد أُطلِع على الموضوع من قبل، وعلى أكمل وجه، حينما كتب ريتشارد كلارك الاستراتيجية القومية لحماية الفضاء السيبراني. لكن ذلك كان قبل أربعة أعوام، ومنذ ذلك الحين كان قد اندلع كثير من الأزمات. لم تكن السيبرانية قط في دائرة اهتمامات الرئيس أكثر من مجرد صورة باهتة ثانوية عابرة.

في عجالة، سرد ماكونيل أهم النقاط التي تعد نتاج عقدين من التحليلات، والثغرات الأمنية في الحواسيب وقابليتها للتعرض للخطر، وتنامي استخدام الحواسيب في كل مناحي الحياة الأمريكية، والدليل النابض الذي قدمه اختبار المولد الكهربائي أورورا الذي كان قد تم قبل ذلك بشهرين فقط. ثم صعَّد ماكونيل من جسامة الأخطار، وصاغ قضيته مستخدما كل ما كان يستطيع حشده من مصطلحات تعبر عن الضرورة والحاجة الملحة، قال ماكونيل: أولئك الإرهابيون التسعة عشر الذين شنوا هجوم الحادي عشر من سبتمبر، إذا كانت لديهم مهارة سيبرانية، وإذا كانوا قد اخترقوا مخدمات أحد البنوك الكبيرة في مدينة نيويورك وأفسدوا ملفاته، لاستطاعوا إحداث أضرار اقتصادية أكثر مما أحدثوا بهدمهم البرجين التوأمين.

استدار بوش نحو وزير الخزانة هنري بولسون، وسأله: هل هذا صحيح يا هانك؟

كان ماكونيل قد ناقش هذه النقطة تحديدا مع بولسون في اجتماع خاص قبل ذلك بأسبوع. أجاب بولسون من خلفية الغرفة: «نعم، سيدي الرئيس». كان النظام المصرفي يعتمد على الثقة، وكان يمكن لهجوم من هذا النوع أن يلحق به ضررا جسيما.

اشتاط بوش، وهب واقفا وسار في أرجاء الغرفة. كان ماكونيل قد وضعه في موقف حرج، إذ أبرز تهديدا واصفا إياه بأنه أكبر من التهديد الذي يثقل ذهنه ويشغل تفكيره هو وكل أمريكي آخر طوال فترة الأعوام الخمسة ونصف العام السابقة، تهديد «حادي عشر من سبتمبر» آخر، وكان قد فعل ذلك أمام أكبر مستشاريه للأمن. لم يستطع بوش أن يدع الأمر يمر فقط.

قال بوش: «ماكونيل، أنت أثرت هذه المشكلة. أمامك ثلاثون يوما لحلها».

إنه كان مطلبا عسيرا يصعب تحقيقه، ثلاثون يوما لحل مشكلة كانت تحوم في الأرجاء وتدور رحاها منذ أربعين عاما. لكنه على الأقل كان قد استحوذ على اهتمام الرئيس. لقد كان في أثناء مثل تلك اللحظات تحديدا - وهي نادرة في

سجلات هذا التاريخ – يجري رسم وتدبير القفزات التي تحرز تقدما في السياسة، مثل: السؤال البريء الذي طرحه رونالد ريغان بعد أن شاهد فيلم «ألعاب الحرب» (المناورات الحربية) «هل يمكن حدوث مثل هذا الأمر في الواقع؟»، أدى إلى أول توجيه رئاسي بشأن أمن الحاسوب؛ في أعقاب تفجيرات مدينة أوكلاهوما سيتي، فإن عقلية الأزمة لدى بيل كلينتون ونزوعه إلى التفكير دائما في أن الأسوأ سيحدث، حفّزا واستحثا تدفقا كبيرا من الدراسات، ومجموعات العمل، وفي نهاية المطاف، تغييرات مؤسسية حقيقية حوّلت الأمن السيبراني إلى قضية عامة رئيسية. الآن، كان ماكونيل يأمل أن يؤدي – ربما- استياء وغضب بوش إلى إطلاق العنان لموجة التغيير الجديدة التالية.

منذ عودته إلى الحكومة، كان ماكونيل يجري دراسة مسحية للمشهد، وكان قد صُدم من ضآلة ما أُحرز من تقدم خلال العقد الذي كان هو في أثنائه بعيدا عن الحياة العامة. كان البنتاغون والفروع العسكرية قد سدت الكثير من الثغرات في شبكاتها، لكن - على الرغم من اللجان، وتجارب نماذج المحاكاة، وجلسات الاستماع في الكونغرس، وحتى المراسيم الرئاسية التي كان ديك كلارك قد كتبها لكل من كلينتون وبوش - لم تختلف الأحوال في أماكن أخرى في الحكومة، ومازالت أكثر من ذلك في القطاع الخاص، ولم تكن أقل عرضة للهجمات السيبرانية.

كانت أسباب هذا المأزق هي أيضا ذاتها ولم تختلف، إذ إن الشركات الخاصة لم تكن ترغب في إنفاق المال على الأمن السيبراني، وأبدت ممانعة تجاه كل اللوائح والتعليمات التي كانت تدفعها إلى فعل ذلك. وفي الوقت ذاته، كانت الدوائر الفدرالية تفتقر إلى النبوغ أو الموارد اللازمة لتنفيذ هذه المهمة، باستثناء وكالة الأمن القومي، التي لم تكن لديها السلطة القانونية ولا الرغبة.

كانت قد استُحدثت كيانات في أثناء موجة الاهتمام الأخيرة، أثناء سطوة كلارك باعتباره منسق السيبرانية في عهد كلينتون وفي أول عامين من عهد بوش، وكان أبرز هذه الكيانات هو المجلس السيبراني المشترك بين الوكالات ومراكز تشارك وتحليل المعلومات التي كانت تقرن الخبراء الحكوميين مع مالكي الشركات الخاصة المعنية بالبنية الأساسية (الشؤون المالية، والطاقة الكهربائية، والنقل، وما إلى ذلك). لكن معظم تلك المشروعات توقفت بعد استقالة كلارك قبل ذلك بأربعة أعوام. الآن، مع

أوامر بوش بالتحرك والمضي قدما، شرع ماكونيل في جمع تلك الكيانات أو استحداث كيانات جديدة، هذه المرة مدعومة بتمويل حقيقي جاد.

أسند ماكونيل المهمة إلى فريق عمل سيبراني مشترك بين الوكالات، تديره إحدى مساعديه، ميليسا هاثاواي Melissa Hathaway، المديرة السابقة لوحدة عمليات المعلومات في شركة «بووز آلين»، التي أحضرها ماكونيل معه لتكون كبيرة مساعديه للسيبرانية في مديرية الاستخبارات القومية.

إن حماية الجانب المدني غير العسكري للحكومة من الهجمات السيبرانية كانت ميدانا جديدا. قبل ذلك بخمسة عشر عاما، حينما بدأت الفروع العسكرية في مواجهة المشكلة، كان أول ما اتخذوه من خطوات هو تزويد حواسيبهم بأنظمة كشف التسلل. لذا، وكخطوة أولى، احتسب فريق عمل «هاثاواي» ما كان سيتطلب الأمر للكشف عن التسلل إلى الشبكات المدنية غير العسكرية، وتبين أن المتطلبات ستكون ضخمة. حينما بدأ الطاقم التقني في قاعدة «كيلي» الجوية في رصد شبكات الحاسوب في منتصف التسعينيات من القرن العشرين، كانت كل مخدمات سلاح الجو عبر البلاد لديها نحو مائة نقطة وصول إلى الإنترنت. أما الآن، فإن جميع وكالات ودوائر الحكومة الفدرالية التي لا حصر لها كان لديها 4300 نقطة وصول.

إضافة إلى ذلك، وبموجب تشريع، أُسندت مهمة تأمين هذه النقاط إلى وزارة الأمن الداخلي، وهي منظمة هجين دمجت معا 22 دائرة كانت قبل ذلك تحت مظلة ثماني وزارات منفصلة. لقد كانت الفكرة جمع كل الدوائر التي لها حتى أدنى مسؤولية عن حماية الأمة من الهجمات الإرهابية وتوحيدها في ديوان وزاري واحد قوي. لكن في الواقع، لم تكن هذه الخطوة سوى تفتيت للسلطة، إذ كانت تثقل كاهل الوزير المسؤول بمهام أكبر من أن يتمكن أي شخص من إدارتها بمفرده، وتدفن في غياهب الأجهزة البيروقراطية القاصية، منظمات كانت قبل ذلك مفعمة بالحيوية، مثل منظومة البنتاغون للاتصالات القومية، التي كانت تدير برامج الإنذار من كل أنواع الهجمات، بما فيها الهجمات السيبرانية. كانت وزارة الأمن الداخلي معزولة ماديا وسياسيا، وكان مقرها محشورا في مجمع صغير بجادة نبراسكا Nebraska Avenue في أقصى شمال غرب واشنطن، على بعد خمسة أميال من البيت الأبيض، وهو المجمع نفسه الذي كانت وكالة الأمن القومي قد حصرت فيه مديرية أمن

المعلومات حتى أواخر الستينيات من القرن العشرين، حينما نُقلت إلى ملحق المطار الذي يبعد نصف ساعة بالسيارة من فورت ميد (أقرب إلى حد ما من جادة نبراسكا التي تستغرق ساعة).

في العام 2004، العام الثاني لعمليات وزارة الأمن الداخلي، ونتاج إحدى مبادرات ديك كلارك، تعاقدت الوزارة على نظام لكشف التسلل على نطاق الحكومة بكاملها، كان يسمى «آينشتاين Einstein». لكن تبدى أن المهمة يتعذر تنفيذها[4]، إذ إن أكبر حاسوب فائق كان سيصعب عليه رصد حركة بيانات تدخل وتخرج عبر أربعة آلاف مدخل إلى الإنترنت. وعلى أي حال لم تكن الدوائر الفدرالية ملزمة بتنصيب النظام.

هذا التباين بين الأهداف والقدرات أدى إلى تمهيد السبيل للبرنامج الجديد الذي أطلقه ماكونيل وهاثاواي، الذي أطلقا عليه اسم «المبادرة القومية الشاملة للأمن السيبراني (سي إن سي آي) Comprehensive National Cybersecurity Initiative (CNCI). كانت هذه المبادرة تدعو إلى إنشاء وكالة فوقية (دائرة عليا) لتعمل على دمج مخدمات الحكومة المتفرقة في «شبكة مؤسسية فدرالية» واحدة، ووضع معايير أمنية صارمة، وتقليص نقاط الدخول إلى الإنترنت من أكثر من أربعة آلاف إلى خمسين نقطة فقط. على أي حال، كان هذا هو الهدف.

في 9 يناير من العام 2008[5]، بعد ثمانية أشهر من جلسة إحاطة ماكونيل الكبيرة، وقَّع بوش على توجيه رئاسي للأمن القومي، «إن إس بي دي - 54» NSPD-54، الذي أشار إلى الأخطار السيبرانية التي تنطوي عليها نقاط الضعف والثغرات الأمنية في أمريكا، مستعينا في كثير من عباراته بما جاء عبر عقد من التوجيهات والدراسات، وأمر بتنفيذ خطة «هاثاواي» باعتبارها العلاج.

في الأسابيع التي سبقت ذلك التوجيه، شدد ماكونيل على أن الخطة ستكون مكلفة. رفض بوش التحذير قائلا إنه على استعداد لإنفاق أموال قدر ما كان فرانكلين روزفلت Franklin Roosevelt قد أنفق على «مشروع مانهاتن». جنبا إلى جنب مع مكتب الموازنة بالبيت الأبيض، وضع ماكونيل خطة خمسية تصل قيمتها إلى 18 مليار دولار، ولم تستقطع لجنة الاستخبارات في الكونغرس منها إلا مبلغا صغيرا، تاركة له 17.3 مليار دولار.

على الرغم من أن المهمة الأساسية للخطة كانت هي حماية شبكات الحاسوب الخاصة بالدوائر المدنية غير العسكرية، فإن البرنامج بكامله – الموازنة التي بلغت عدة ملايين من الدولارات، ونص التوجيه الرئاسي للأمن القومي «إن إس بي دي - 54»، حتى وجود شيء يدعى «المبادرة القومية الشاملة للأمن السيبراني» - خُتمت جميعا بخاتم سري جدا. مثل معظم القضايا السيبرانية، كانت الخطة مرتبطة ارتباطا وثيقا بالغموض التعتيمي لوكالة الأمن القومي، ولم يكن هذا من قبيل المصادفة، إذ إنه على الورق، كانت وزارة الأمن الداخلي هي الدائرة المناطة بها المبادرة، لكن وكالة الأمن القومي كانت مسؤولة عن الدعم التقني؛ ولأن وزارة الأمن الداخلي - أو أي دائرة أخرى - لم تكن تمتلك المعرفة أو الموارد لتنفيذ ما جاء في توجيه الرئيس، فإن بؤرة السلطة لهذا البرنامج أيضا، كانت ستميل من مجمع جادة نبراسكا إلى المجمع المترامي الأطراف في فورت ميد.

أيضا، كان مدير وكالة الأمن القومي كيث ألكسندر، جهبذا ضليعا في سياسات الموازنة أكثر من المديرين في وزارة الأمن الداخلي. كان يعرف، مثلما كان مايك هايدن قبله، أي التشريعات تخول أي مجموعات من الأنشطة (الباب الخمسين للاستخبارات، الباب العاشر للعمليات العسكرية، الباب الثامن عشر للتحقيقات الجنائية)، وأيا من لجان الكونغرس تبت في تمويل كل منها. لذا، حينما قُسمت موازنة المبادرة البالغة 17.3 مليار دولار بين الدوائر المختلفة، ذهب الجزء الأكبر منها إلى وكالة الأمن القومي التي كانت ستضطلع في نهاية المطاف بمهمة شراء وصيانة الأجهزة والمعدات، وهي أكثر عناصر البرنامج تكلفة. حدد الكونغرس أن تنفق فورت ميد حصتها من المبلغ على الدفاع السيبراني. لكن، تعريف هذا المصطلح كان فضفاضا، وكانت موازنة وكالة الأمن القومي على درجة عالية من السرية، لذلك خصص ألكسندر الأموال وفقا لما رآه مناسبا.

في أثناء ذلك، حدَّثت وزارة الأمن الداخلي «آينشتاين»[6]، نظام كشف عن التسلل القاصر، إلى «آينشتاين 2»، الذي صُمم ليس فقط لكشف أي نشاط ضار على الشبكة، ولكن أيضا لإرسال تنبيه تلقائي. بدأت الوزارة وضع الإطار النظري المفاهيمي لنظام «آينشتاين 3»، الذي - مجددا، من الناحية النظرية – كان سيصد المتسللين بشكل تلقائي وعلى نحو مؤلل. تحملت وكالة الأمن القومي هذه المشروعات

باعتبار ذلك جزءا من حصتها في الموازنة التي بلغت 17.3 مليار دولار، ودمجتها مع المشروعات الضخمة لجمع البيانات وطحنها وغربلتها التي كانت الوكالة قد أطلقتها بالفعل. لكن بعد فترة وجيزة من تضافر الجهود حول مشروع «آينشتاين»، تراجع ألكسندر، معللا ذلك بأن متطلبات الوكالات المدنية (غير العسكرية) ونهج وزارة الأمن الداخلي، لم تكن تتوافق مع وكالة الأمن القومي. بقي مقاولو (متعهدو) «آينشتاين» التجاريون في العمل، وعيَّنت وزارة الأمن الداخلي فريقا من المتخصصين في السيبرانية، لكنهم تُركوا لشأنهم، وكان عليهم البدء من جديد. تعثر البرنامج، ولم يحقق أهدافه، ودخل في حالة من الاختلال الوظيفي والانهيار.

وهكذا، على الرغم من التزام الرئيس الكامل وأكوام الأموال، فإن الثغرات الأمنية للحواسيب وقابليتها للتعرض للهجوم، وتداعيات ذلك على الأمن القومي، والعافية الاقتصادية، والتماسك والوئام الاجتماعي - وهو موضوع كان قد أثار أجراس الإنذار بين الفينة والأخرى خلال العقود الأربعة السابقة - كان ينحرف مجددا نحو التهاون والتقصير.

كان ألكسندر لايزال ملزما بإنفاق حصته من المال على الدفاع السيبراني، لكن في هذا الوقت، فإن ما أدركه كين مينيهان من حقيقة أن الهجوم السيبراني والدفاع السيبراني يعملان على تكنولوجيا واحدة، ومترادفان من الناحية العملية، كان متأصلا تماما في فكر ومعتقد فورت ميد.

كانت المفاهيم الأساسية للسيبرانية - مهاجمة شبكة الحاسوب، وحماية شبكة الحاسوب، واستغلال شبكة الحاسوب - لاتزال في مرحلة الذيوع. لكن البطاقة الرابحة كانت، ودائما كانت، هي الاستغلال، استغلال شبكات الحاسوب هو فن وعلم العثور على الثغرات الأمنية في شبكة الخصم واستغلالها، والولوج إلى داخلها، والتلاعب بها. كان استغلال شبكات الحاسوب يمكن اعتباره، واستخدامه، وتبريره على أنه تحضير لهجوم سيبراني مستقبلي، أو على أنه أحد أشكال ما كان خبراء الاستراتيجية قد وصفوه منذ فترة طويلة بأنه «الدفاع الإيجابي» active defense، وهو النفاذ إلى شبكة الخصم لمعرفة أنواع الهجمات التي كان يخطط لها، حتى تستطيع الوكالة ابتكار أسلوب لتعطيلها، أو إضعافها، أو دحرها على نحو وقائي استباقي.

كان ألكسندر يعمم وينشر مقولة[7] أن «الدفاع الإيجابي» هو أمر أساسي وضروري، مثلما هي الحال في الأنواع الأخرى من وسائل الحرب، إذ إن المعادل السيبراني لـ «خط ماجينو» Maginot Line(*) أو «سور الصين العظيم» Great Wall of China (**) ما كان يعتمد على المدى الطويل. كان الخصوم سيجدون طريقة للمناورة حول الموانع أو القفز عليها. لذا، في المجالس المشتركة بين الوكالات، وفي الإدلاء بالشهادة خلف الأبواب المغلقة، كان ألكسندر يوضح أن هذا الجزء من «المبادرة القومية الشاملة للأمن السيبراني» كان ينبغي أن يركز على استغلال شبكات الحاسوب. بطبيعة الحال، حالما يجري الإنفاق بسخاء على أدوات استغلال شبكات الحاسوب، فإنه من الممكن برمجتها للهجوم والدفاع، لأن استغلال شبكات الحاسوب كان عنصر تمكين مساعد لكليهما. حينما كان ألكسندر يفحص البريد الإلكتروني وينفذ في شبكات الهاتف الجوال للمتمردين العراقيين، كان ذلك استغلالا لشبكة الحاسوب؛ أما حينما منحه الرئيس بوش الإذن بتعطيل وعرقلة تلك الشبكات - لاعتراض وإرسال رسائل مزيفة ينتهي بها الأمر إلى قتل المتمردين - كان ذلك مهاجمة لشبكة الحاسوب «سي إن أيه». باستثناء الخطوة الأخيرة، أي قرار الهجوم، فإن استغلال شبكات الحاسوب ومهاجمة شبكات الحاسوب كانا متطابقين.

كانت هذه هي طبيعة التكنولوجيا أيا كانت نوايا أي أحد (وكانت نوايا ألكسندر واضحة)، مما جعل السيطرة على الأمر على نحو صارم لزاما على القادة السياسيين، لضمان أن السياسة هي التي كانت تشكل استخدام التكنولوجيا، وليس العكس. لكن، بينما لم تكد الأدوات السيبرانية تُدمج مع أسلحة الحرب، وبينما كانت شبكات الحاسوب تدير تقريبا كل أوجه الحياة اليومية، تزحزحت السلطة على نحو غير ملحوظ، ثم على نحو مفاجئ، إلى أساطين التكنولوجيا في فورت ميد.

(*) خط ماجينو Maginot Line الذي يعد نموذجا للتحصينات الدفاعية الثابتة، كان خطا من التحصينات الأسمنتية، والعقبات، ومنشآت الأسلحة، بنتها فرنسا في الثلاثينيات لردع أي غزو من ألمانيا وإجبار الألمان على التحرك حول التحصينات. سمي على اسم وزير الحرب الفرنسي أندريه ماجينو André Maginot الذي نادى للأخذ بنظرية الدفاع الثابت ودافع عنها أمام البرلمان الفرنسي. [المترجم].

(**) سور الصين العظيم Great Wall of China هو عبارة عن سلسلة من التحصينات المصنوعة من الحجر، والطوب، والخشب، وغيرها من المواد، بُني بشكل عام على طول خط من الشرق إلى الغرب عبر الحدود الشمالية التاريخية للصين لحماية الدول والإمبراطوريات الصينية ضد غارات وغزوات مجموعات البدو المختلفة من ذوي التطلعات التوسعية. [المترجم].

أتت اللحظة المحورية الحاسمة[8] في هذا التحول في مقر وكالة الأمن القومي، في الساعة الثانية والنصف بعد ظهر يوم الجمعة 24 أكتوبر من العام 2008، إذ لاحظ فريق من محللي استخبارات الإشارة (سيجينت) شيئا غريبا يحدث في شبكات القيادة المركزية للولايات المتحدة، المقر الرئيسي لإدارة الحروب في أفغانستان والعراق.

كانت أداة إرشادية تنبيهية (بيكون) تطلق إشارة، وبدا أنها قادمة من داخل الحاسوب السري للقيادة المركزية. لم يكن هذا الأمر غريبا فقط، بل كان من المفترض أنه مستحيل الحدوث، إذ إن الشبكات العسكرية المصنفة على أنها سرية لم تكن متصلة بالإنترنت العام، فالشبكتان معزولتان تماما بوجود «فجوة هوائية» air gap[*] بينهما، وكما قال عنها الجميع، لم يكن من الممكن أن يجتازها حتى قراصنة الحاسوب الأكثر حنكة. لكن، بطريقة ما، توصل أحد إلى هذا وحقن بضعة أسطر من التعليمات البرمجية (الكود) الخبيثة الضارة بأحد خطوط الاتصال العسكرية الأكثر أمنا. كان هذا هو المصدر الوحيد المقنع للأداة الإرشادية التنبيهية (البيكون).

بقدر ما كان الجميع يعرف، كانت هذه هي المرة الأولى، التي تُخترق فيها شبكة في وزارة الدفاع مصنفة على أنها سرية.

ربما لم يكن قد رُصد هذا التسلل، بيد أنه قبل عام من ذلك، حينما انطلقت الحرب السيبرانية باعتبارها ظاهرة تسود العالم بأسره، فإن ريتشارد شيفر Richard Schaeffer، رئيس مديرية ضمان المعلومات في وكالة الأمن القومي - الذي كان أفراد طاقمه يقضون أيام عملهم منكبين على دراسة وفحص واختبار أساليب جديدة يستخدمها شخص من الخارج لخرق دفاعاتها - كان يحلم بتحقيق هدف جديد. على مدار العقد السابق، كانت الفروع العسكرية ومختلف فرق العمل المشتركة قد أدّت عملا جيدا على نحو معقول لحماية المحيط الخارجي لشبكاتها. لكن ماذا لو فاتهم شيء ما، وكان هناك خصم داخل الشبكة بالفعل، غير مكتشف، ومختبئ بين آلاف أو ملايين الملفات، ينسخ محتوياتها أو يفسدها؟

أسند شيفر مهمة فحص الشبكات المصنفة على أنها سرية إلى فريقه الأحمر - الوحدة ذاتها التي كانت قد أجرت مناورة تدريب «المتلقي المؤهل» في العام 1997.

(*) وهو يعني أن جهاز حاسوب أو شبكة مفصولة كهربائيا (بفجوة هوائية تخيلية) من جميع الشبكات الأخرى. [المترجم].

اكتشف هذا الفريق الأداة الإرشادية التنبيهية، كانت مرفقة بفيروس حاسوبي متنقل (دودة الحاسوب) كانوا قد رأوها قبل ذلك بعامين تحت عنوان agent.btz. كانت أداة راقية متميزة، إذ إنها بعد النفاذ إلى الشبكة وتفحص البيانات، كانت الأداة الإرشادية التنبيهية مبرمجة لتحملها جميعا عائدة إلى مصدرها. منذ عهد بعيد، كان «مكتب عمليات الولوج المصممة وفقا للحاجة» (تاو - تي إيه أوو)، وهو ورشة لعمليات الحقائب السوداء (العمليات السرية) السيبرانية في وكالة الأمن القومي، قد ابتكر أداة مماثلة.

حمل شيفر الأخبار إلى ألكسندر، وفي غضون خمس دقائق توصل الرجلان وفريقاهما إلى حل. كانت الأداة الإرشادية التنبيهية مبرمجة للعودة إلى مصدرها؛ لذا، قالوا: دعونا ندلف إلى داخل الأداة الإرشادية التنبيهية ونعيد توجيهها إلى مصدر آخر مختلف؛ على وجه التحديد، أحد صناديق التخزين في وكالة الأمن القومي. بدت الفكرة واعدة. أسند ألكسندر المهمة إلى فريقه التقني، وفي غضون بضع ساعات توصلوا إلى كيفية تصميم البرمجية، وبحلول صباح اليوم التالي كانوا قد أنشأوا البرنامج. بعد ذلك اختبروه على أحد الحواسيب في «فورت ميد»، في البداية حقنوا الفيروس الحاسوبي المتنقل (دودة الحاسوب) agent.btz، ثم بعد ذلك سحبوا الأداة باستخدام تعليمات إعادة التوجيه، وكان الاختبار ناجحا.

كانت الساعة الثانية والنصف من بعد ظهر يوم السبت. في غضون أربع وعشرين ساعة فقط، كانت وكالة الأمن القومي قد توصلت إلى الحل، وبنائه، والتحقق منه. أطلقوا على العملية اسم «اليانكي صائد الظباء» Buckshot Yankee.

في تلك الأثناء، كانت الفروع التحليلية للوكالة تتعقب مسارات الفيروس الحاسوبي المتنقل إلى نقطة بدايته. تكهنوا بأن أحد رجال أو نساء جيش الولايات المتحدة في أفغانستان كان قد اشترى ناقلة بيانات (وحدة ذاكرة فلاشية) مصابة ببرامج خبيثة ضارة وأدخلها إلى حاسوب آمن. (تأكدت هذه الفرضية من تحليل مفصل أُجري على مدار الأشهر القليلة اللاحقة). كانت ناقلات البيانات (وحدات الذاكرة الفلاشية) تُباع على نطاق واسع في الأكشاك في العاصمة الأفغانية كابول، بما في ذلك تلك الأكشاك الموجودة بالقرب من المقر العسكري لحلف شمال الأطلسي (الناتو). اتضح أن روسيا ورّدت كثيرا من ناقلات البيانات تلك، بعضها كان مبرمجا مسبقا بواسطة أحد أجهزة

الاستخبارات، على أمل أن بعض الأمريكيين سيفعل في يوم من الأيام ما كان بعض الأمريكيين قد قاموا به بالفعل، والذي بدا الآن جليا.

لكن كل هذا كان تفاصيل. كانت الصورة الكبيرة الأشمل هي أنه في صباح يوم الإثنين بعد بدء الأزمة، كان المسؤولون في البنتاغون يسعون جاهدين من أجل فهم أبعاد وحجم المشكلة، بينما قبل ذلك بيومين، كانت وكالة الأمن القومي قد حلتها.

دعا الأدميرال مايك مولين Mike Mullen، رئيس الهيئة المشتركة لرؤساء الأركان، إلى عقد اجتماع طارئ صباح يوم الإثنين لمناقشة إجراءات العمل، بيد أنه وجد أن قادة الفروع لم يرسلوا سوى ضباط برتبة كولونيل (عقيد) لحضور الاجتماع. وكاد يصرخ «ماذا أنتم فاعلون هنا؟». إن شبكات قيادة الحرب التي تخوضها الأمة جرى المساس بها وتعرضت لما يثير الشبهة؛ لم يكن ممكنا كسب المعارك من دون الثقة بتلك الشبكات. كان مولين بحاجة إلى التحدث مع القادة، ومع مديري العمليات بهيئة الأركان المشتركة والاستخبارات، وهذا يعني أنه كان بحاجة إلى التحدث مع جنرالات من فئة ثلاث وأربع نجوم وضباط برتبة أدميرال (لواء بحري).

في وقت لاحق من صباح ذلك اليوم، رتب مولين اجتماعا عبر الهاتف مع مايك ماكونيل، وكيث ألكسندر، والجنرال كيفن تشيلتون Kevin Chilton، رئيس القيادة الاستراتيجية للولايات المتحدة، التي كانت تضم مقر «فريق العمل المشترك لعمليات الشبكة العالمية»، أحدث تجسيد للمكاتب ذات الهيكل الفضفاض التي كانت قد أُنشئت في بادئ الأمر، قبل عقد من الزمان، مثل «فريق العمل المشترك لحماية شبكات الحاسوب».

بدأ مولين المحادثة بالسؤال ذاته الذي كان جون هامري قد طرحه من قبل في العام 1998، في أعقاب عملية «الشروق الشمسي»، أول تغلغل عميق للشبكات العسكرية: من الذي يتولى زمام الأمور؟

على مدار خمسة وعشرين عاما، منذ أن وقَّع رونالد ريغان على أول توجيه رئاسي بشأن أمن الحاسوب، فإن البيت الأبيض، والبنتاغون، والكونغرس، و«فورت ميد»، ومختلف مراكز وسائل حرب المعلومات في الخدمات العسكرية، كانوا متعارضين ومتنازعين بشأن هذا السؤال. الآن، أصر الجنرال تشيلتون على أنه هو الذي كان مسؤولا، نظرا إلى أن القيادة الاستراتيجية كانت تضم «فريق العمل المشترك لعمليات الشبكة العالمية».

سأل مولين: «ثم ما الخطة؟».

سكت شيلتون للحظة وقال: «قل له يا كيث».

من الجلي أن القيادة الاستراتيجية لم يكن لديها شيء. لم يكن أي كيان، مدني أو عسكري، لديه أي شيء - أي أفكار بشأن من الذي فعل هذا، وكيف يمكن إيقافه، وما الذي ينبغي فعله بعد ذلك - باستثناء الوكالة التي لديها معظم التمويل، والتكنولوجيا، والنبوغ للتعامل مع مثل هذه الأسئلة، وكالة الأمن القومي.

كان مديرو وكالة الأمن القومي في أثناء العقد الماضي قد عملوا على نحو محموم من أجل الحفاظ على بقاء «فورت ميد» في مواجهة منافسة المكاتب السيبرانية العشوائية المبعثرة بالخدمات العسكرية - «الحفاظ على الغموض»، مثلما كان بيل بيري قد وصف المهمة إلى كين مينيهان. كان أفضل أسلوب للقيام بذلك هو تقديم المبررات، يوما بعد يوم، وإثبات صواب أن وكالة الأمن القومي كانت هي المكان الوحيد الذي كان يعرف كيفية قيامه بهذا النوع من الأشياء، وهذا هو ما صوّره ألكسندر على نحو مثير مع عملية «اليانكي صائد الظباء».

بمزيج من الارتياع والحيرة، كان بوب غيتس يراقب هذا التناقض بين سيطرة «فورت ميد» وتدافع البنتاغون وتخبطه. لقد كان غيتس وزيرا للدفاع طوال ما يقرب من العامين، بعد تاريخ مهني طويل في وكالة الاستخبارات المركزية، وفترة قصيرة كان قد قضاها في البيت الأبيض في أثناء فترة ولاية بوش الأب، وكان يواصل التعجب من الخلل الوظيفي الشديد في الجهاز الإداري للبنتاغون. عند بداية توليه المنصب[9]، كانت القوات المسلحة في خضم حربين، كلتاهما تجري على نحو سيئ جدا. مع ذلك، كانت طائفة واسعة من كبار الضباط الموجودين في البناية يتصرفون كأن العالم يعيش في سلام، إذ إنهم كانوا يدفعون بالأسلحة ذاتها باهظة الثمن، التي بُنيت من أجل حرب أسطورية كبرى في المستقبل، ذات الأسلحة التي كانوا يدفعون بها منذ الحرب الباردة، ويرقون النوع نفسه من الضباط الذين يؤدون التحية العسكرية بقرقعة حماسية، ويلتزمون بالحضور إلى العمل في مواعيد منضبطة - باختصار، لم يكونوا يفعلون أي شيء ذا فائدة – حتى فصل غيتس بضعة جنرالات من الخدمة، واستعاض عنهم بضباط بدا أنهم قادرون على، وراغبون في، مساعدة الرجال والنساء على القتال، والموت، والإصابة بجروح بالغة في الحروب التي كانت دائرة حينذاك.

كان غيتس منذ مجيئه إلى البنتاغون، قد سمع في كل يوم تقريبا، إحاطات بشأن آخر محاولة للنفاذ إلى شبكات وزارة الدفاع قام بها أحد الخصوم الخطرين، أو أحد قراصنة الحاسوب المخربين. كان هذا هو الانتهاك الخطير جدا الذي كان قد حذّر الكثيرين من أنه ربما يحدث؛ ومع ذلك، مازال الجميع يؤدون مناورات وألاعيب بيروقراطية. لم يكن يبدو أن أحدا قادر على تمييز ما هو جلي.

إن مايك ماكونيل، الذي كان على وفاق مع غيتس منذ فترة توليه منصب مدير وكالة الأمن القومي، طرح مرارا وتكرارا أمر القيادة السيبرانية الموحدة، التي كانت ستقوم مقام كل مكاتب السيبرانية المتناثرة، وتدير العمليات الهجومية والدفاعية (لأنهما تنطويان على ذات التكنولوجيا، والأنشطة، والمهارات)، ومثاليا أن تكون كائنة في «فورت ميد» باعتبارها مقرا لها (لأنه هناك كانت تحتشد التكنولوجيا، والأنشطة، والمهارات). دعم ماكونيل حجته بجزء من المعرفة ببواطن الأمور، إذ إن وكالة الأمن القومي لم تكن ترغب في تشارك المعلومات الاستخباراتية مع قادة العمليات؛ السبيل الوحيد لأن يحدث ذلك هو صهر مدير وكالة الأمن القومي وقائد السيبرانية في شخص واحد.

لطالما كان غيتس يعتقد أن فكرة ماكونيل تبدو منطقية، وعملية «اليانكي صائد الظباء» أوضحت الأمر بجلاء تام.

ثمة تطور آخر غلّف هذا الأمر بالشعور بالضرورة والحاجة الملحة. كان الوقت يمضي على فترة ولاية ألكسندر لوكالة الأمن القومي. كان معظم المديرين قد خدم ثلاثة أعوام، وكان ألكسندر قد مكث في منصبه ثلاثة أعوام وشهرين. بعيدا عن الحساب، كان غيتس قد سمع شائعات بأن ألكسندر كان يعتزم التقاعد، ليس فقط من الوكالة، ولكن أيضا من الجيش الميداني (القوات البرية). فكر غيتس أن هذا سيكون كارثيا، إذ إن وكالة الاستخبارات المركزية كانت قد توقعت أخيرا هجوما سيبرانيا كبيرا في غضون العامين المقبلين. ها نحن في أزمة أقل حجما لكنها على الرغم من ذلك خطيرة، وكان ألكسندر هو المسؤول الوحيد الذي كان يمسك بزمام ما كان يحدث.

جرت العادة على أن يكون مدير وكالة الأمن القومي جنرالا من فئة الثلاث نجوم أو أدميرالا؛ وأن يكون قادة القوات العسكرية من فئة الأربع نجوم. توصل غيتس

إلى أن إحدى وسائل توحيد السياسة السيبرانية والإبقاء على ألكسندر هي استحداث قيادة سيبرانية جديدة، وكتابة مرسومها بحيث يكون قائدها هو أيضا مدير وكالة الأمن القومي (مثلما كان ماكونيل قد اقترح)، ويضع ألكسندر في المنصب المزدوج، وبذلك يمنحه نجمة رابعة، وثلاثة أعوام أخرى على الأقل في المنصب.

وفي واقع الأمر، كانت إشاعات رحيل ألكسندر الوشيك غير صحيحة. بالمصادفة، قبل وقت قصير من عملية «اليانكي صائد الظباء»، حدد ألكسندر موعدا للحصول على إحاطة معلومات بشأن التقاعد، والتي كان الجنرالات ملزمين بالحصول عليها عند اكتسابهم النجمة الثالثة. كان ألكسندر قد أجل جلسته لأشهر عدة، كانت هذه الأشياء عادة مضيعة للوقت، وهو كان مشغولا. وأخيرا، ضغطت عليه قيادة شؤون ضباط الجيش الميداني؛ لذلك، ذهب لحضور الجلسة المقررة التالية.

بعد ذلك بيومين تلقى ألكسندر اتصالا هاتفيا من غيتس، كان يريد أن يعرف منه ما إذا كانت إشاعات تقاعده صحيحة. أكد له ألكسندر أن الأمر ليس كذلك. أيضا، أخبره غيتس بخطة جلب نجمة رابعة له.

كان الأمر سيستغرق عدة أشهر لتسوية الأمور في البنتاغون، والأوساط الاستخباراتية، والكونغرس. في تلك الأثناء، جرت الانتخابات، ووصل الرئيس الجديد باراك أوباما إلى البيت الأبيض. لكن غيتس، الذي وافق على البقاء في منصب وزير الدفاع لمدة عام على الأقل، دفع بالفكرة إلى الأمام قدما. في 23 يونيو من العام 2009[10]، وقّع مذكرة، آمرا باستحداث قيادة سيبرانية للولايات المتحدة.

في أثناء العام الأخير من فترة رئاسة بوش والأشهر القليلة الأولى من عهد أوباما، كان غيتس يتصارع مع معضلة. كان قد أدرك منذ فترة أنه حينما يتعلق الأمر بالأمن السيبراني، ليس هناك بديل عن «فورت ميد». إن فكرة تحويل وزارة الأمن الداخلي إلى وكالة أمن قومي للبنية الأساسية المدنية غير العسكرية، وهو الهاجس الذي كان البعض في البيت الأبيض لايزال يرعاه، كانت أضغاث أحلام. لم يكن لدى وزارة الأمن الداخلي الأموال، أو القوى البشرية، أو المقدرة التقنية، وعمليا على نحو واقعي، لن يكون لديها أي من ذلك. لكن لأن وكالة الأمن القومي من الناحية القانونية (وعلى نحو محكم) محظور عليها المراقبة المحلية، فهي أيضا لم تكن تستطيع حماية البنية الأساسية المدنية غير العسكرية.

في 7 يوليو من العام 2010 كان غيتس يتناول طعام الغداء[11] في البنتاغون مع جانيت نابوليتانو Janet Napolitano، وزيرة الأمن الداخلي، لاقتراح وسيلة للخروج من هذا الدغل. كانت الفكرة هي أن نابوليتانو كانت ستسمي نائبا ثانيا لمدير وكالة الأمن القومي (من الناحية الرسمية، كان سينبغي أن يسمي غيتس الشخص، ولكنه سيكون من اختيارها)، وفي حالة وجود تهديد للبنية الأساسية الحرجة في البلاد، سيكون في إمكان هذا النائب الجديد أن يستعين بالموارد التقنية لوكالة الأمن القومي في حين يتذرع بالسلطة القانونية لوزارة الأمن الداخلي.

أعجبت نابوليتانو بالفكرة. في اجتماع لاحق، أعدا مذكرة تفاهم بشأن هذا الترتيب، تضمنت مذكرة التفاهم مجموعة من الدروع الوقائية لحماية الخصوصية والحريات المدنية. كان غيتس ونابوليتانو قد تشاورا مع الجنرال ألكسندر الذي وافق على الفكرة وباركها. في 27 يوليو، بعد أقل من ثلاثة أسابيع من غدائهما الأول، حمل غيتس ونابوليتانو الفكرة إلى الرئيس أوباما. لم يكن لدى أوباما اعتراضات، ومررها إلى توماس دونيلون Thomas Donilon، مستشاره للأمن القومي، الذي محّصها مع لجنة مشتركة بين الوكالات تابعة لمجلس الأمن القومي.

كان كل شيء يبدو على المسار الصحيح. ترك غيتس ونابوليتانو التفاصيل لمعاونيهما وعادا إلى الأعمال الأكثر ضرورة وإلحاحا.

على مدى الأشهر القليلة اللاحقة، كُشف عن الاتفاق.

قبل تفويض الأمر، اختارت نابوليتانو مرشحها لمنصب نائب المدير للسيبرانية، وهو أدميرال من فئة النجمتين يدعى مايكل براون Michael Brown، كان يشغل في وزارتها منصب نائب وزير مساعد للأمن السيبراني. بدا براون مثاليا لهذه المهمة، كان قد درس الرياضيات وعلم التشفير في الأكاديمية البحرية، وعمل في فرق استخبارات الإشارة في وكالة الأمن القومي، وفي أواخر التسعينيات من القرن العشرين انتقل إلى البنتاغون كأحد المحللين في تحقيقات اختراقات «الشروق الشمسي» وعملية «متاهة ضوء القمر» في «فريق العمل المشترك لحماية شبكات الحاسوب». حينما أقنع مايك ماكونيل الرئيس بوش بإنفاق 18 مليار دولار على الأمن السيبراني، طلب من براون أن يعمل في وزارة الأمن الداخلي، للمساعدة على حماية الشبكات المدنية بالطريقة ذاتها التي كان قد ساعد بها على حماية الشبكات العسكرية. على مدار العامين اللاحقين،

كان هذا ما يحاول براون تنفيذه، موسعا فريق السيبرانية في وزارة الأمن الداخلي من ثمانية وعشرين شخصا إلى ما يقرب من أربعمائة، وحوَّل فريق الاستجابة لطوارئ الحاسوب إلى تنظيم وظيفي بعض الشيء. إذا كان هناك أحد يستطيع دمج ثقافتي وكالة الأمن القومي ووزارة الأمن الداخلي، فمن المرجح أن يكون هو مايك براون.

لذلك السبب، وعلى الرغم من ذلك، كان براون يواجه عقبات في كل خطوة. كان نائب نابوليتانو، «جين هول لوت»Jane Holl Lute - وهو محام، ومساعد سابق للسكرتير العام للأمم المتحدة لدعم حفظ السلام، ورجل جيش ميداني مخضرم في استخبارات الإشارات – يرتاب بشدة في وكالة الأمن القومي، وممانعا لأي خطة كان من شأنها أن تمنح الوكالة أي سلطة في الشؤون المحلية، أو ربما تحول الإنترنت إلى «ساحة حرب»[12]. وهذا كان ينطبق أيضا على مستشار البيت الأبيض للأمن السيبراني، هوارد شميت Howard Schmidt، الذي كان يفزع وينفر ممن كانوا يصفون الفضاء السيبراني على أنه «ميدان»، بالمفهوم ذاته الذي كان ضباط سلاح الجو يصفون به السماء، وضباط سلاح البحرية يصفون به المحيطات على أنها «ميادين» للعمليات العسكرية. إن رتبة براون باعتباره ضابطا في سلاح البحرية، وخلفيته في علم التشفير، وخبرته مع وكالة الأمن القومي، كانت جميعها تشير إلى أن هذا المسعى المشترك سيكون بعيدا عن الشراكة المتكافئة؛ لذلك، فإن «فورت ميد» هي التي كانت ستدير الأمور.

أيضا، كانت هناك ممانعة فيما بين نواب الوزراء الأعضاء في مجلس الأمن القومي، كان بعضهم متكدرا من أن هذه الصفقة قد سارت من دون تشاور معهم. في نهاية المطاف، وافقوا على أن يكون براون[13] هو «منسق الأمن السيبراني»، لكنهم لم يكونوا ليوافقوا على أن يكون نائبا لمدير وكالة الأمن القومي، ولم يكونوا ليمنحوه السلطة القانونية التي كان سيحتاجها للقيام بالمهمة المتوخاة التي كان غيتس ونابوليتانو قد تخيلاها.

وعلى الرغم من أن عددا قليلا فقط كانوا يتذكرون هذا الزمن البعيد، فإن الأمر كان يعيد إلى الأذهان النزاع الذي نشب منذ أكثر من ربع قرن، في العام 1984، حينما عارض المدافعون عن الحريات المدنية في الكونغرس الخطة المبينة في توجيه الرئيس ريغان، «إن إس دي دي145-» NSDD-145 (التوجيه الرئاسي السري المتعلق بالأمن

القومي)، لأنها كانت تضع المعايير القياسية لأمن الحاسوب في أيدي لجنة يديرها مدير وكالة الأمن القومي.

عمليا، كانت الاجتماعات التي تضم موظفي وزارة الأمن الداخلي ومجلس الأمن القومي تغلي من التوتر. كانت خطة غيتس-نابوليتانو تدعو كل دائرة إلى إرسال عشرة محللين إلى مقر الدائرة الأخرى بوصفها نوعا من تبادل الثقافات. منذ البداية، أرسلت «فورت ميد» محلليها العشرة، تسعة من مجلس الأمن القومي، ومحللا واحدا من القيادة السيبرانية؛ لكن وزارة الأمن الداخلي كانت بطيئة في التجاوب. كان جزء من المشكلة هو الأمور اللوجستية العادية. كان يعمل في وكالة الأمن القومي خمسة وعشرون ألف شخص، ولم تكن مبادلة عشرة منهم أمرا يتطلب تضحية كبيرة. لكن وزارة الأمن الداخلي لم يكن لديها سوى بضع مئات من المتخصصين في السيبرانية، فبدلا من نقل أي منهم، قرر لوت توظيف عشرة أشخاص جدد، وهو تدبير كان ينطوي على تلاعب بحسابات الموازنة، وفحص لاستخراج التصاريح الأمنية، باختصار، كان تدبيرا يحتاج إلى وقت، كثير من الوقت. لكن، قبل وقت كافٍ من انضمام الأشخاص العشرة، تعثر الترتيب، وكاد يصل إلى طريق مسدود.

في 31 أكتوبر من العام 2010 رفعت القيادة السيبرانية للولايات المتحدة علمها على «فورت ميد»، مع تولي الجنرال ألكسندر القيادة، بالتزامن مع دخوله عامه السادس مديرا لوكالة الأمن القومي التي كانت تعج بقوى سياسية، وبيروقراطية، وحوسبية لم يسبق لها مثيل.

11

«كومة القش بكاملها»

في العام 2007، أثناء الأسابيع الأولى من فترة تولي مايك ماكونيل منصب مدير الاستخبارات القومية، أطلعه أحد مساعديه على لوحة أعدتها شركة «فيريساين» VeriSign، الشركة التي كانت تدير «نظام اسم النطاق» (domain name system)، الذي كان يوثِّق «دوت-كوم» dot-com، و«دوت-جوف» dot-gov، و«دوت-نيت» dot-net، وعناوين البريد الإلكتروني الأخرى التي كانت تجعل الإنترنت تعمل وتؤدي وظيفتها. كانت اللوحة تبين خريطة العالم، ليس من خلال جغرافية كتلة اليابسة والمحيطات، ولكن من خلال أنماط وكثافات سعة قناة الاتصال (عرض النطاق

«في الوقت الذي تُعترَض فيه رسالة البريد الإلكتروني أو محادثة الهاتف الجوال الخاصة بأحد الإرهابيين، كان يُلتقَط أيضا جزء من دردشة الأمريكيين الأبرياء»

الترددي) للشبكة. وفقا لهذه الخريطة فإن 80 في المائة من الاتصالات الرقمية في العالم كانت تمر عبر الولايات المتحدة(*).

كان لهذا آثار كبيرة في الاستخبارات. إذا تبادل أحد الإرهابيين في باكستان رسائل البريد الإلكتروني، أو تحدث على هاتف جوال، مع أحد موردي الأسلحة في سورية، وإذا وجهت الشبكة العالمية اتصالاتهم عبر الولايات المتحدة، فلن يكون هناك حاجة إلى إنشاء محطة معادية لتَفَحُّص وجمع البيانات في منطقة؛ كانت وكالة الأمن القومي تستطيع ببساطة التنصت على تيار البيانات فيها من داخل الولايات المتحدة.

لكن كان هناك عقبة قانونية. في السابق، في السبعينيات من القرن العشرين، كشفت جلسات الاستماع التي ترأسها السناتور فرانك تشيرش Frank Church عن تعسف وإساءة استخدام للسلطة على نطاق واسع من قبل وكالة الاستخبارات المركزية ووكالة الأمن القومي، ينطوي على مراقبة مواطنين أمريكيين، لاسيما النقاد السياسيين والناشطين المناهضين للحرب، في انتهاك حقوقهم ضد «التفتيش والضبط التعسفي غير المبرر» المنصوص عليها في التعديل الرابع للدستور. أدت جلسات الاستماع إلى إصدار «قانون مراقبة الاستخبارات الأجنبية»[1] (Foreign Intelligence Surveillance Act) في العام 1978 الذي حظر المراقبة المحلية من دون برهان لمسوِّغ مقنع مرجح أن الهدف كان عميلا لقوى أجنبية، وأن أماكن المراقبة كانت، أو كانت ستكون، مستخدمة بواسطة ذلك العميل؛ وحتى في هذه الحالة كان سيتعين على الحكومة تقديم الدليل على السبب المسوّغ المقنع المرجح إلى محكمة سرية مختصة بقانون مراقبة الاستخبارات الأجنبية، التي كان سيُعيَّن قضاتها من قبل رئيس المحكمة العليا في الولايات المتحدة. كان الرئيس يمكنه أن

(*) في أواخر التسعينيات من القرن العشرين، حينما بدأ ريتشارد كلارك في إجراء بحث بشأن الثغرات الأمنية في البنية الأساسية وقابليتها للتعرض للهجوم، علم أن 80 في المائة من حركة بيانات الإنترنت على مستوى العالم كانت تمر عبر بنايتين فقط في الولايات المتحدة، كانت إحداهما تسمى «إم أيه إي غرب» (MAE West)، (إم أيه إي MAE تعني: مبدل المنطقة المتروبوليتية (الحضرية) الكبرى Metropolitan Area Exchange) في مدينة سان هوزيه بولاية كاليفورنيا، والبناية الأخرى كانت تسمى «إم أيه إي شرق» (MAE East)، فوق مطعم اللحم المشوي في «تايسونس كورنر» Tysons Corner بولاية فيرجينيا Virginia. في إحدى الليالي اصطحب كلارك أحد عملاء الخدمة السرية لتناول العشاء في مطعم اللحم المشوي، وبعد تناول العشاء ألقيا نظرة على الحجرة في الطابق العلوي. (أحضر كلارك العميل معه ليتجنب إلقاء القبض عليه). لقد صدم الاثنان لمدى سهولة أن يتمكن أي مخرب من أن يسبب أضرارا كارثية مدمرة.

يمنح سلطة المراقبة من دون أمر من المحكمة، لكن فقط إذا أقر المدعي العام تحت القسم بأن الهدف كان يُعتقد أنه عميل أجنبي، وأن التنصت لم يكن سيلتقط اتصالات «أحد أفراد الولايات المتحدة»، الذي يعرف على أنه مواطن أمريكي، أو أحد المقيمين بصفة دائمة، أو إحدى المؤسسات.

بعد هجمات الحادي عشر من سبتمبر(2) في العام 2001، على نحو متعجل مرر الكونغرس قانون مكافحة الإرهاب (أو قانون الوطنية)، الذي عَدّل ونَقّح - من بين أمور أخرى - «قانون مراقبة الاستخبارات الأجنبية» للسماح بمراقبة عملاء أجانب، وأعضاء في مجموعات إرهابية غير محددة المعالم، مثل تنظيم «القاعدة»، الذي لا ينتمي إلى أي دولة قومية.

في رأي ماكونيل كان «قانون مراقبة الاستخبارات الأجنبية» - حتى مع ذلك التنقيح - متقادما وعفّى عليه الزمن وبحاجة إلى التغيير. في العصر الرقمي لم تعد هناك أماكن منفصلة قائمة بذاتها لتراقَب، كان الفضاء السيبراني في كل مكان. كذلك لم تكن الحكومة تستطيع أن تقر صراحة بأنه في الوقت الذي تُعترَض فيه رسالة البريد الإلكتروني أو محادثة الهاتف الجوال الخاصة بأحد الإرهابيين، كان يُلتقَط أيضا جزء من دردشة الأمريكيين الأبرياء. كانت هذه هي طبيعة حزم البيانات التي كانت تخلط أجزاء من اتصالات كثيرة وتدفعها عبر المسار الأكثر كفاءة. ولأن المسار الأكثر كفاءة كان عادة يمر عبر الولايات المتحدة فسيكون من الصعب عدم التقاط بعض بيانات الأمريكيين أثناء العملية.

كان ماكونيل يُحضِر معه الخريطة التي أعدتها شركة «فيريساين»، في جلسات إحاطة الرئيس، وفي اجتماعاته مع معاونيه لشؤون الأمن القومي، وفي جلسات غير رسمية مع أعضاء الكونغرس، وكان يشرح ويبين تداعياتها وآثارها، وكان يروِّج لتعديل «قانون مراقبة الاستخبارات الأجنبية».

عرف ماكونيل أنه كان يحرز تقدما حينما التقى مع جاك مورثا Jack Murtha، الديموقراطي البارز في اللجنة الفرعية للاعتمادات المالية المخصصة للدفاع التابعة لمجلس النواب. كان مورثا يبلغ من العمر سبعة وسبعين عاما، وكان يقضي فترته السابعة عشرة في الكونغرس، كان مورثا سببا في أن مر ماكونيل بأوقات عصيبة في التسعينيات من القرن الماضي، حينما كان ماكونيل مديرا لوكالة

الأمن القومي. عند مرحلة ما هدد مورثا بإنهاء برامج الوكالة الخاصة بوسائل حرب المعلومات، لاسيما تلك التي كانت تميل إلى الهجومية. لكن خريطة شركة «فيريساين» لفتت انتباهه على نحو آسر.

قال ماكونيل وهو يشير إلى نتوء عند منطقة أمريكية: «انظروا أين يوجد كل عرض النطاق الترددي (سعة قناة الاتصال)»، «نحن بحاجة إلى تغيير القانون لمنحنا إمكانية الوصول». بلع مورثا الطعم وتقبل الفكرة، وكذلك كان تقريبا جميع من سمع ذلك.

لم يكن الرئيس بوش بحاجة إلى مناشدة خاصة. من منطلق حرصه على عمل أي شيء قد يؤدي إلى اصطياد إرهابي متلبس بالجرم المشهود، وجد بوش في خريطة «فيريساين» مسوغا منطقيا لأن يتخذ إجراء، وأمر فريقه القانوني بإعداد مسودة مشروع قانون.

في 28 يوليو، في خطابه الإذاعي الأسبوعي ليوم السبت، أعلن بوش أنه كان سيرسل مشروع القانون إلى الكونغرس. قال إنه في عصر الهواتف الجوالة والإنترنت صارت القوانين الحالية «متقادمة جدا»[3]؛ ونتيجةً لذلك، «نحن نفقد قدرا كبيرا ومؤثرا من المعلومات الاستخباراتية الأجنبية التي كان علينا جمعها لحماية بلدنا».

بعد مضي أربعة أيام طرح زعماء الجمهوريين في مجلس الشيوخ مشروع القانون على المجلس بوصفه «قانون حماية أمريكا» (Protect America Act). حقق القانون كل ما كان ماكونيل يرغب في أن يفعله. أشارت إحدى الفقرات الرئيسية في القانون إلى أن «المراقبة الإلكترونية» لأحد الأمريكيين[4] لن تكون غير مشروعة – لم تكن ستُعرَّف حتى على أنها «مراقبة إلكترونية» - إذا استهدفت شخصا كان «يُعتقد على نحو مرجح أنه موجود خارج الولايات المتحدة». من ثم فإن التجميع المتعدي الطائش لبيانات الأمريكيين، الأمر الحتمي الذي لا يمكن تجنبه في العالم الرقمي، كان بذلك سيُعفى من احتمال الملاحقة القضائية. أوضحت مادة أخرى من القانون أنه بموجب هذا القانون الجديد فإن توثيق المدعي العام أمام محكمة قانون مراقبة الاستخبارات الأجنبية «ليس مطالبا بتحديد مرافق، أو أماكن، أو مقرات أو ممتلكات معينة»، حيث كانت المعلومات الاستخباراتية ستُجمَع. مثلما كان ماكونيل يقول مرارا وتكرارا فإن أهداف المراقبة في العصر الرقمي - بخلاف تلك التي كانت في عصر التنصت على الهواتف – لم تعد تشغل حيزا ماديا.

ثمة فقرة أخرى مهمة وذات دلالة نصت على أن الحكومة لم تكن تستطيع الحصول على هذه المعلومات إلا «بمساعدة مزود خدمة اتصالات». كان هذا الشرط الاحترازي بالكاد ملحوظا، وعلى هذا النحو، بدا كأنه قيد، لكنه في الواقع منح وكالة الأمن القومي ترخيصا باسترجاع البيانات من الشركات الخاصة، وأعطى الشركات غطاء قانونيا للتعاون مع وكالة الأمن القومي. كانت بضعة أطراف خارجية تعرف أن مزودي الخدمات، مثل: «ويسترن يونيون» Western Union و«أيه تي آند تي» AT&T في الأيام السالفة، إلى «سبرينت» Sprint و«فيريزون» Verizon في حقبة الشركات التي عُرفت باسم «بابي بيلز» Baby Bells(*)، إلى «مايكروسوفت» Microsoft، و«غوغل» Google، وغيرهما من رواد عصر الإنترنت الآخرين، كانوا قد تمتعوا وقتا طويلا بترتيبات واتفاقات ذات منفعة متبادلة مع وكالة الأمن القومي ومكتب التحقيقات الفدرالي. كان هذا القسم من مشروع القانون سيستحوذ على اهتمام كبير، وسيثير جدلا هائلا، بعد ستة أعوام لاحقة، حينما كشفت تسريبات «إدوارد سنودن» Edward Snowden عن مدى اتساع نطاق هذه الترتيبات.

باستثناء شرط التشاور مع محكمة قانون مراقبة الاستخبارات الأجنبية ولجان الكونغرس المختارة، وكل منها كانت تُعقد في سرية، كان القيد الوحيد الذي وضعه مشروع القانون على المراقبة هو أن البيانات التي كان يُحصَل عليها عن الأمريكيين – الذين عادة ما كانت اتصالاتهم تنجرف مع حزم البيانات الخاضعة للمراقبة - كان يتعين «التقليل منها إلى أدنى حد». كان هذا يعني أنه لم يكن باستطاعة الحكومة تخزين أسماء أي أمريكيين، أو محتويات اتصالاتهم حفاظا على الخصوصية والحريات المدنية، وبدلا من ذلك لا يُخزَّن سوى أرقام هواتفهم، وتاريخ، وتوقيت، ومدة المحادثة. قليلون ممن قرأوا مشروع القانون هم الذين فهموا تعريف «التقليل إلى أدنى حد» أو أدركوا مقدار ما كان يمكن أن يكشفه حتى هذا القدر من المعلومات - البيانات الواصفة، كما كان يطلق عليها - بشأن هوية شخص ما، وما يفعله من أنشطة.

(*) «بابي بيلز» Baby Bells: هي شركات الهاتف الإقليمية الأمريكية التي شُكِّلت من تفكك «أيه تي آند تي» AT&T في العام 1984. أُنشئت «بابي بيلز» بسبب دعوى مكافحة الاحتكار التي أقامتها وزارة العدل الأمريكية ضد شركة الهاتف والتلغراف الأمريكية. [المترجم].

بعد يومين من المداولة والنقاش وافق مجلس الشيوخ على هذا الإجراء بنسبة 60 مقابل 28. في اليوم التالي أيد مجلس النواب بنسبة 227 مقابل 183. في اليوم التالي، 5 أغسطس من العام 2007، بعد ثمانية أيام فقط من خطابه الإذاعي، وقّع الرئيس بوش على مشروع القانون ليصير قانونا.

مع أوجه التقدم التقني في العقد السابق - برنامج «تيربلانس» (صخب)، و«بوابة الوقت الحقيقي الإقليمية» (آر تي آر جي) ، والجيل الجديد من الحواسيب فائقة القدرة، وبراعة مخترقي الحواسيب في «مكتب عمليات الولوج المصممة وفقا للحاجة» (تاو - تي إيه أوو) - كانت الحكومة تستطيع الخوض في كل تيارات بيانات شبكة الويب العالمية. وبفضل القوى السياسية الجديدة المخولة إلى «فورت ميد» – دمج كل مكاتب استخبارات الإشارات في الفروع العسكرية، وابتداء القيادة السيبرانية للولايات المتحدة برئاسة مدير وكالة الأمن القومي - كانت وكالة الأمن القومي هي التي ستقوم بذلك الخوض، بموافقة وتفويض البيت الأبيض، والكونغرس، والغرفة السرية التي كانت المحكمة العليا قد أقامتها كـمفوض لها في العالم المعتم.

كان عصرا جديدا من الآفاق الرحبة لوكالة الأمن القومي، وكان كيث ألكسندر هو الرحالة المثالي لها. كان الانتقاد الذائع لإخفاق الاستخبارات في الحادي عشر من سبتمبر، هو أن الدوائر المعنية كانت تمتلك الكثير من الحقائق - الكثير من نقاط البيانات - التي ربما كانت تشير إلى هجوم وشيك، لكن لم يستطع أحد أن «يربط النقاط» بعضها ببعض[5]. الآن، بعد ستة أعوام لاحقة، سمحت تكنولوجيات جديدة بأن تُجمِّع وكالة الأمن القومي هذا الكم الكبير من البيانات – تيارا من نقاط البيانات الذي يتدفق بسلاسة – إلى درجة أن النقاط كانت تقريبا هي بذاتها تصل بعضها ببعض.

إن تضافر أوجه التقدم التكنولوجي وما حدث بعد الحادي عشر من سبتمبر من مخاوف من الإرهاب، أفرز تغيرا ثقافيا أيضا، إذ حدث قبول متزايد، وإن كان إلى حد ما خضوعا وإذعانا، للتدخلات في الحياة اليومية. في السابق في العام 1984 كان أول توجيه رئاسي بشأن أمن الحاسوب الذي وقّعه رونالد ريغان، قد أُلغي لأنه كان يمكِّن وكالة الأمن القومي من وضع معايير قياسية لكل الحواسيب الأمريكية – العسكرية،

والحكومية، والخاصة، والتجارية - ولم يكن الكونغرس ليسمح بأن يكون لـ «فورت ميد» رأي في المراقبة أو السياسة الداخلية. الآن، بعد مضي ما يربو على ربع قرن، كانت البيانات الرقمية تعبر الحدود على نحو اعتيادي. من الناحية العملية تلاشت الحدود وكذلك تلاشى ما كان على وكالة الأمن القومي من قيود جغرافية.

في هذا السياق رأى ألكسندر مدخلا لإحياء برنامج البيانات الواصفة الذي كان قد أنشأه قبل ذلك في بداية العقد، بوصفه رئيسا لقيادة استخبارات وأمن الجيش الميداني (القوات البرية) في «فورت بيلفوار». من الناحية المنطقية بدت مسألة إحياء برنامج البيانات الواصفة مناسبة للاتجاهات التقنية، والسياسية، والثقافية. لنفترض أن ألكسندر كان سيتذرع بأنه بينما يجري تتبع الاتصالات الأجنبية، رصد رجال عمليات استخبارات الإشارة (سيجينت) رقم هاتف أمريكيا يتصل برقم هاتف أحد الإرهابيين المعروفين في باكستان. كانت وكالة الأمن القومي تستطيع أن تطلب الحصول على تفويض من محكمة قانون مراقبة الاستخبارات الأجنبية لاكتشاف المزيد بشأن هذا الأمريكي. ربما يجدون أنه من المفيد أيضا معرفة أرقام الهواتف الأخرى التي كان المشتبه فيه الأمريكي قد اتصل بها، ثم ربما يجري تتبع الأرقام التي كان هؤلاء الأشخاص قد اتصلوا بها. وتماما مثل تجربة «بيلفوار»، ولكن بصورة أوضح وعلى نطاق أكبر، فإن الأمر لم يكن سيستغرق وقتا طويلا حتى تكون وكالة الأمن القومي قد خزنت بيانات عن ملايين من الناس، والكثير منهم أمريكيون ليس لهم أي علاقة فعلية بالإرهاب.

ثم جاء تحريف حديث. عند نقطة ما، استمرت حجة ألكسندر، ربما يكتشف محللو استخبارات الإشارة بعض الأمريكيين المتورطين في نشاط مريب فعلي. هم ربما يرغبون في تتبع هذا الشخص عدة أشهر، وربما أعواما، حتى يمكنهم البحث في البيانات عن نمط تهديدات، لربما تكون هناك صلة بين متآمرين، وتعقبها ليستدل بها على جذورها. من ثم كان من المنطقي تفحُّص وجمع وتخزين كل شيء بشأن كل شخص. غيّر محامو وكالة الأمن القومي حتى بعض التعريفات البسيطة الواضحة، بحيث لا يعتبر هذا الفعل «جمع» بيانات عن مواطنين أمريكيين، لأن ذلك كان سيعد غير مشروع، إذ إنه بموجب المصطلحات الجديدة، كانت وكالة الأمن القومي لا تضطلع إلا بتخزين البيانات. لم يكن الجمع ليحدث إلى أن يسترجع أحد المحللين

البيانات من الملفات، وهذا أمر لم يكن ليحدث إلا باستصدار الموافقة القانونية الملائمة من محكمة قانون مراقبة الاستخبارات الأجنبية.

بموجب «قانون مراقبة الاستخبارات الأجنبية»، لا يمكن تخزين البيانات إلا إذا كانت تعتبر «ذات صلة» بتقصٍ متعلق باستخبارات أجنبية أو إرهاب. لكن بموجب هذا التعريف الجديد، كان من المحتمل أن يكون كل شيء ذا صلة، إذ لم يكن هناك سبيل لمعرفة ما الذي يكون ذا صلة إلا بعد أن يصير ذا صلة؛ لذلك ينبغي أن يكون لديك كل شيء بين يديك لإجراء تقييم شامل قاطع. إذا كان كثير من المعلومات الاستخباراتية ينطوي على البحث عن إبرة في كومة قش، مثلما كان ألكسندر يروق له أن يقول، فينبغي أن يكون لديك إمكان الوصول إلى «كومة القش بكاملها»[6].

جرى استحداث محكمة قانون مراقبة الاستخبارات الأجنبية للموافقة على - أو رفض، أو تعديل - طلبات محددة لجمع البيانات؛ من ذلك المنطلق، هي كانت أشبه بمحكمة بلدية ابتدائية أكثر منها محكمة عليا. لكن في هذه الحالة، أصدرت محكمة قانون مراقبة الاستخبارات الأجنبية حكما بشأن تفسير وكالة الأمن القومي الفضفاض للقانون، وهي اعتمدت هذا التعريف لتعبير «ذي صلة».

كانت لدى كيث ألكسندر كومة القش بكاملها.

كانت تلك هي حال الفضاء السيبراني، شبكة ويب يجري تمشيطها، وتجريفها، والنفاذ إليها بواسطة أجهزة الاستخبارات في جميع أرجاء العالم، لاسيما الأجهزة الأمريكية، حينما خفت حدة السباق الرئاسي نحو البيت الأبيض بين السناتور باراك أوباما والسناتور جون ماكين، في خريف العام 2008.

كان الرئيس بوش ملزما بتقديم إفادات استخباراتية لكلا المرشحين؛ لذا، في 12 سبتمبر، أوفد دمايك ماكونيل لإحاطة أوباما، المرشح الديموقراطي، في مقر حملته الانتخابية في شيكاغو Chicago. كان بوش حذرا من هذا الإجراء برمته، ووجَّه ماكونيل، قبل مغادرته، إلى ألا يفصح عن أي شيء بشأن العمليات في أفغانستان والعراق، وألا يطلع إلا المرشح ذاته، وليس أي أحد في فريقه.

اثنان من أعضاء فريق أوباما، كان من المقرر حضورهما لتسجيل ملاحظات، شعرا بالاستياء، وكذلك شعر المرشح، حينما طلب منهما مدير الاستخبارات مغادرة الجلسة؛ لكن الجلسة استمرت على نحو ودي بما فيه الكفاية، إذ قال أوباما إنه لم

يكن يرغب في أن يسمع أي شيء بشأن العراق أو أفغانستان، كانت لديه أفكاره الخاصة بشأن تلك الحروب؛ أما ما كان يرغب حقا في مناقشته فهو الإرهاب.

استعرض ماكونيل التهديدات التي كان يشكلها تنظيم القاعدة والجماعات المنتسبة إليه، والمؤامرات المختلفة في داخل البلاد وخارجها، والتي لم يُعَرْقل سوى بعضها فقط، وبشق الأنفس. كان أوباما مبهورا، وهو كان عضوا حديث العهد في لجنة العلاقات الخارجية بمجلس الشيوخ، لكنه لم يكن استمع قط لمثل هذه الإحاطة التفصيلية من مثل هذا المسؤول الاستخباراتي رفيع المستوى. عند هذه النقطة، كان قد مرت خمسون دقيقة، وهي فترة أطول مما كان معاونو أوباما قد خططوا له، لكن أوباما كان مستقرا متأقلما وسأل ماكونيل بشأن ما لديه في سجل الإحاطة عدا ذلك.

سعيدا بأداء التزاماته، أخبر مدير المخابرات الرئيس المقبل بشأن موقف خطة كوريا الشمالية لتفجير قنبلة ذرية، وبرنامج إيران لبناء قنبلة ذرية، ومفاعل سورية النووي في الصحراء (كانت إسرائيل قد قصفته قبل ذلك بعام، لكن «الأسد» كان لايزال على اتصال بموردي المفاعل في «بيونغ يانغ»). استغرق هذا عشرين دقيقة أخرى. أخبره أوباما بأن يستأنف حديثه.

وهكذا، وتماما مثلما كان ماكونيل قد فعل حينما وافق بوش على خطة الهجوم السيبراني على العراق بعد عشر دقائق من بدء اجتماع كان مجدولا له أن يمتد ساعة، عرج ماكونيل على الموضوع الذي يسبب له عميق القلق. في وقت سابق في أوائل العام، كان مسؤولون رسميون بالولايات المتحدة قد حذروا أوباما وماكين من أن الصين كانت قد اخترقت أنظمة الحاسوب الخاصة بحملتيهما الانتخابيتين، وقلبوها رأسا على عقب بحثا عما يخصهما من أوراق تبين موقفيهما تجاه قضايا معينة، وموارد مالية، ورسائل البريد الإلكتروني.

قال ماكونيل: «لقد استغلوا النظام الخاص بك». «ماذا لو كانوا قد دمروه؟».

أجاب أوباما: «كان ذلك سيسبب مشكلة لي».

استطرد ماكونيل، وتمهيدا لفكرته الأساسية: «تخيل أنه كان في استطاعتهم تدمير بنيتنا الأساسية الحرجة».

قال أوباما، مدركا ما الذي كان المدير يقصده، كأنه يكمل عبارة ماكونيل: «كان ذلك سيسبب مشكلة للأمة».

قال ماكونيل: «ذلك هو الخطر»، ثم دخل إلى ختامه المحبوك الذي تدرب عليه جيدا، وإنذاره بشأن أوجه الضعف والثغرات الأمنية في البلاد، ومقدرة العديد من القوى على استغلالها، وليس الصين فقط.

في الختام، طلب أوباما من ماكونيل أن يأتي ليراه مجددا في الأسبوع الأول من فترته الرئاسية.

في الواقع، تقابل ماكونيل مع أوباما بعد ذلك في مكتبه الانتقالي، في 8 ديسمبر، فيما بين انتصاره في ليلة الانتخابات ويوم تنصيبه. أحضر ماكونيل معه معاونته ميليسا هاثاواي، التي عرضت بإيجاز الخطوط العريضة لـ «المبادرة القومية الشاملة للأمن السيبراني» (سي إن سي آي) التي كانت قد كتبتها للرئيس بوش، لكن لم تنفذ بعد. طلب منها أوباما أن تبدأ التفكير بشأن إجراء «مراجعة الستين يوما» a sixty-day review للسياسة السيبرانية للولايات المتحدة.

أصاب المراجعة تأخير طفيف. لم تكن السيبرانية هي القضية العاجلة والأكثر إلحاحا في جدول أعمال الرئيس الجديد. بداية، أمر أوباما معاونا آخر في حملته، وهو محلل سابق في وكالة الاستخبارات المركزية يدعى بروس ريدل Bruce Riedel، بأن يكتب مراجعة الستين يوما لسياسة الولايات المتحدة في أفغانستان. ثم كانت هناك مسألة إيجاد حل لانهيار القطاع المصرفي، وتداعي صناعة السيارات، أسوأ أزمة اقتصادية منذ الكساد الاقتصادي الكبير(*).

مع ذلك، في التاسع من فبراير[7]، بعد ثلاثة أسابيع فقط من ولايته، وليس متأخرا كثيرا عن الجدول الزمني، أعلن أوباما على الملأ مراجعة الستين يوما للسيبرانية، وقدم هاثاواي على أنها رئيس لها. استغرقت المراجعة أكثر من ستين يوما[8]، لاستكمالها استغرق الأمر 109 أيام، لكن في 29 مايو أصدرت هاثاواي ومجموعتها المشتركة بين الوكالات وثيقة تتألف من اثنتين وسبعين صفحة، بعنوان «مراجعة لسياسة الفضاء السيبراني .. ضمان بنية أساسية للمعلومات والاتصالات تتسم بالموثوقية

(*) الكساد الاقتصادي الكبير هو عبارة عن كساد اقتصادي عالمي شديد وقع خلال فترة الثلاثينيات من القرن العشرين، بداية من الولايات المتحدة. تباين توقيت الكساد الكبير عبر الدول؛ في معظم البلدان بدأ في العام 1929 واستمر حتى أواخر الثلاثينيات. كان أطول وأعمق وأوسع انتشار للركود في القرن العشرين. بدأ الكساد الاقتصادي الكبير في الولايات المتحدة بعد انخفاض كبير في أسعار الأسهم بدأ في 4 سبتمبر من العام 1929، وأصبح أخبارا عالمية مع انهيار سوق البورصة في 29 أكتوبر من العام 1929 (المعروف باسم الثلاثاء الأسود). [المترجم].

والقدرة على التكيف» Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.

على نحو غريب، بدا التقرير مثل[9] التقارير، والمراجعات، والتوجيهات التي كانت قد صدرت قبله، بل حتى أشار إلى العديد منها بالاسم، من بينها التوجيه الرئاسي للأمن القومي «إن إس بي دي - 54» NSPD-54 الذي أصدره بوش، والاستراتيجية القومية لحماية الفضاء السيبراني، وتقرير «مارش»، وبضع دراسات عن مجلس علوم الدفاع، وجلسات استماع السناتور نان. لم يكن هناك إلا قدر ضئيل من الجديد الذي يمكن أن يقال بشأن الموضوع؛ لكن بعض الأشياء القديمة كان قد سبق اعتمادها وتبنيها رسميا، لذا لم يكن أحد قد سمع بها خارج زمرة الخبراء الذين كانوا قد تابعوا المراحل طوال أعوام أو عقود؛ ومن ثم، فإن إعادة هاثاواي سرد المشكلات القديمة نفسها، وأساليب علاجها، لم تكن تكرارا زائدا على الحاجة، ولا لزوم له.

مجددا، من ثم، اشتمل التقرير على استهلال يشير إلى الوجود المطلق للفضاء السيبراني وانتشاره في كل مكان، وما فيه من «أوجه ضعف وثغرات أمنية استراتيجية»، وينطوي على «أخطار بالغة» تهدد «البنية الأساسية الحرجة» و«المعلومات العسكرية الحساسة». احتوى التقرير على القليل بشأن «السلطات المتداخلة» بين الدوائر الفدرالية، والحاجة إلى «حوار وطني»، و«خطة عمل» من أجل «تشارك المعلومات» مع «الشراكات بين القطاعين العام والخاص». وأخيرا، قدم التقرير اقتراحا بتعيين «مسؤول لسياسة الأمن السيبراني» في البيت الأبيض، المنصب الذي افترضت هاثاواي أنها كانت ستشغله، تماما مثلما نصَّب ديك كلارك نفسه «المنسق القومي» في وثيقة مماثلة كان قد قدمها إلى بيل كلينتون.

لكن، هاثاواي اصطدمت بعقبات منذ البداية. كانت هاثاواي شقراء، جذابة، تبلغ من العمر نحو أربعين عاما، لكن موظفي البيت الأبيض كانوا يستخفون بها بوصفها «خشنة» (شائكة) و«حازمة بجرأة»... هجاء لاذع يشيع رمي النساء به لسلوك كان سيمكن تحمله في الرجال، باعتباره سلوكا عدوانيا جريئا فقط، أو حتى طبيعيا، وربما يكون هذا السلوك في الرجال مثيرا للإعجاب. من المؤكد أن هاثاواي كانت أقل حدة وحزما من كلارك، لكن كلارك كان خبيرا في سياسات وصراعات

المكاتب، يسعى إلى مصادقة من يحمونه ويدافعون عنه في أعلى المناصب والحلفاء في كل أرجاء الجهاز الإداري. لم يكن لدى هاثاواي سوى شخص واحد يحميها ويدافع عنها، هو مايك ماكونيل، وحينما استبدله أوباما في الأسبوع الأول من رئاسته، باتت من دون غطاء.

كانت هناك مشكلة أخرى، مشكلة كان كلارك أيضا قد واجهها. أشارت مراجعة هاثاواي إلى أن الشركات الخاصة تمتلك معظم مسارات الفضاء السيبراني، ومن ثم كان لزاما عليها «تقاسم المسؤولية»[10]، من أجل تأمينها، وهو التوجه الذي أثار مخاوف انعكاسية من اللوائح الحكومية، التي لاتزال هي الكلمة الأسوأ بين المسؤولين التنفيذيين في «وادي السليكون». انحاز مستشار أوباما الاقتصادي الأرعن، لورنس سومرز Lawrence Summers، إلى الصناعة في هذا النزاع، وأصر على أنه ينبغي عدم تقييد قاطرات النمو الاقتصادي، لاسيما في أثناء ما كان قد أصبح يطلق عليه «الركود العظيم» (كذلك، فقد كان سومرز، باعتباره وزيرا للخزانة في عهد كلينتون، هو أبغض الناس إلى كلارك، حينما حاول الضغط من أجل اللوائح).

تعثرت هاثاواي وحقيبة ملفاتها التي تضطلع بها بين بروز الشواغل الاقتصادية وعزلتها الإدارية. لقد غادرت في أغسطس، وكانت مهمشة قبل ذلك التاريخ بوقت طويل.

لكن أوباما لم يتجاهل مخاوف هاثاواي. في 29 مايو، وهو اليوم نفسه الذي أصدرت فيه هاثاواي مراجعتها، تحدث أوباما لمدة سبع عشرة دقيقة في الغرفة الشرقية للبيت الأبيض بشأن الفضاء السيبراني، ومكانته المركزية في الحياة الحديثة، و«هذا التهديد السيبراني»[11] على أنه «واحد من أخطر تحديات الاقتصاد والأمن القومي التي تواجهها الأمة».

لم يكن يتحدث فقط وفقا لنص مكتوب، ولكن أيضا من واقع تجربته الشخصية. ولد أوباما في العام 1961، قرب نهاية طفرة المواليد baby boom (بخلاف بوش وكلينتون اللذين ولدا قبله بخمسة عشر عاما في بداية الطفرة)، كان أوباما هو أول رئيس أمريكي يتصفح الفضاء السيبراني في حياته اليومية (حينما طلبت منه الخدمة السرية أن يتخلى عن جهاز «بلاك بيري» BlackBerry الخاص به لأسباب أمنية، عارض أوباما؛ وكحل وسط، فإن مديرية ضمان المعلومات في وكالة الأمن القومي

صنعت له جهاز بلاك بيري فريدا من نوعه، مزودا بأحدث ما توصل إليه العلم في تقنيات التشفير، والحماية، وبضع خدع أخرى على درجة عالية من السرية)؛ وكان أوباما هو أول رئيس تُختَرَق سجلات حملته من قوى أجنبية. فهم أوباما الأخطار.

لكن شيئا آخر أثار مخاوفه. قبل بضعة أيام من تنصيبه، كان الرئيس بوش قد أطلعه على عمليتين سريتين كان يأمل أن يستكملهما أوباما. كانت إحداهما تتعلق بضربات سرية باستخدام الطائرات المسيرة من دون طيار ضد مقاتلي القاعدة في باكستان. والأخرى تشتمل على حملة هجوم سيبراني محكمة التنظيم وجسورة على نحو مذهل، أطلق عليها اسم حركي هو «عملية الألعاب الأولمبية»، عُرفت فيما بعد باسم «ستاكسنت» Stuxnet، بهدف إبطاء وإعاقة ما بدا أنه برنامج أسلحة نووية في إيران.

بعد فترة وجيزة من الإحاطة الموجزة التي قدمها مايك ماكونيل، بشأن قابلية أمريكا للتعرض للهجمات السيبرانية، كان هذا الإفصاح قد أضاء مصباحا يختلف عن ذلك الذي كان يومض على نحو متقطع فقط في رؤوس الرؤساء، وكبار المسؤولين، والمستشارين الذين كانوا قد تعرضوا لهذا الموضوع في العقود السابقة. إنه كان الوجه الآخر للدرس الدارج المألوف، وهو: ما يستطيع العدو أن يفعله بنا في يوم ما، نستطيع أن نفعله بالعدو الآن.

12

«لقد عبر أحدهم روبيكون»

«بينما كان الإيرانيون يعملون على إصلاح المفاعل، أعدت وكالة الأمن القومي الجرعة المدمرة الأكثر ديمومة»

أحاط جورج دبليو بوش بنفسه[1] باراك أوباما بشأن «عملية الألعاب الأولمبية»، بدلا من ترك المهمة لأحد مسؤولي الاستخبارات، لأنها، مثل جميع العمليات السيبرانية، كانت تتطلب تصريحا رئاسيا. بعد أدائه اليمين الدستورية، كان لزاما على أوباما إما تجديد البرنامج صراحة وإما التغاضي عن الأمر وتركه ينتهي. لذلك، قدم بوش ذريعة قوية لدفعه إلى الأمام قدما. أخبر خليفته بأن البرنامج قد يعني الفارق بين الحرب مع إيران وفرصة السلام معها.

كانت عملية الألعاب الأولمبية قد بدأت [2]قبل ذلك ببضعة أعوام، في العام 2006، في منتصف فترة بوش الرئاسية الثانية، حينما اكتُشف علماء

إيرانيون يعملون على تركيب أجهزة طرد مركزي - وهي الأرياش الفضية الطويلة التي تخضخض غاز اليورانيوم وتصدمه بسرعة تفوق سرعة الصوت - في أحد المفاعلات النووية في مدينة نطنز Natanz. كان الهدف المعلن هو توليد الطاقة الكهربائية، ولكن إذا رُتبت أجهزة الطرد المركزي في تتالٍ على نحو متعاقب بكميات كبيرة بما يكفي، ولزمن طويل بما فيه الكفاية، فإن العملية ذاتها كان يمكن أن تصنع مواد الأسلحة النووية.

كان نائب الرئيس، تشيني، يؤيد شن غارات جوية على مفاعل نطنز، مثلما فعلت بعض الجهات الإسرائيلية، التي اعتبرت احتمال أن تكون إيران مسلحة نوويا يشكل تهديدا لوجود إسرائيل. ربما كان بوش قد أخذ بهذه الفكرة قبل ذلك ببضعة أعوام، لكنه كان قد ضاق ذرعا من تشدد تشيني الذي لا يلين. كان بوب غيتس Bob Gates، وزير الدفاع الجديد، قد أقنع بوش بأنه سيكون ضارا بالأمن القومي خوض حرب ضد دولة مسلمة ثالثة، في حين أن الاثنتين الأخريين في أفغانستان والعراق مازالتا مستعرتين. لذلك، كان بوش يبحث عن «خيار ثالث»، شيء ما بين الغارات الجوية والوقوف مكتوفي الأيدي من دون فعل شيء.

جاءت الإجابة من «فورت ميد»، أو على نحو أكثر دقة، من التاريخ الممتد على مدار عقود من الدراسات، وتجارب نماذج المحاكاة، والمباريات الحربية (المناورات)، ومشاركات حقيقية سرية في وسائل الحرب المضادة للقيادة والسيطرة، ووسائل حرب المعلومات، ووسائل الحرب السيبرانية، التي كانت كل ابتكاراتها ومنفذيها في الوقت الحالي متمركزة في فورت ميد.

مثل معظم المفاعلات، كان تشغيل مفاعل نطنز يحدث من بُعد من خلال عناصر تحكم (ضوابط) حاسوبية. وبحلول ذلك الوقت، كان ذائعا أن هذه الضوابط يمكن اختراقها والتلاعب بها في هجوم سيبراني - في غضون بضعة أشهر، كان سيُثبت ذلك من خلال «اختبار المولد الكهربائي أورورا» في مختبر «أيداهو» القومي.

من هذا المنطلق، اقترح كيث ألكسندر، مدير وكالة الأمن القومي، شن هجوم سيبراني على عناصر تحكم (ضوابط) مفاعل نطنز.

بالفعل، كانت فرق استخبارات الإشارة (سيجينت) التابعة له قد اكتشفت أوجه ضعف وثغرات أمنية في الحواسيب التي كانت تتحكم في تشغيل المفاعل، وكانوا

قد تجولوا خفية عبر شبكتها، واستطلعوا أبعادها، ووظائفها، وخصائصها، واكتشفوا مزيدا من أوجه الضعف والثغرات الأمنية. كان هذا هو التجسس في العصر الرقمي، «استغلال شبكة الحاسوب» (سي إن إي). من ثم، لم يتطلب الأمر موافقة الرئيس. بالنسبة إلى الخطوة التالية، مهاجمة شبكة الحاسوب (سي إن أيه)، كان بدؤها سيتطلب إذنا رسميا من القائد الأعلى. استعدادا للضوء الأخضر، وضع ألكسندر أساسيات الخطة.

كانت فرق استخبارات الإشارة (سيجينت) التابعة لوكالة الأمن القومي، في أثناء عملياتها التجسسية[3]، قد اكتشفت أن البرمجية المستخدمة للتحكم في أجهزة الطرد المركزي بمفاعل نطنز، صممتها شركة سيمنز Siemens، وهي شركة ألمانية كبرى كانت تُصنِّع «وحدات تحكم منطقية قابلة للبرمجة» (programmable logic controllers) لنظم صناعية في جميع أنحاء العالم. كان التحدي هو ابتكار فيروس حاسوبي متنقل (دودة حاسوب) ليصيب نظام نطنز من دون إصابة أي من أنظمة سيمنز الأخرى في أي مكان آخر، في حالة ما إذا انتشر الفيروس الحاسوبي المتنقل (دودة الحاسوب)، مثلما كانت تفعل الفيروسات الحاسوبية المتنقلة (دودة الحاسوب) في بعض الأحيان.

كان بوش فاقدا للأمل وفي حاجة ماسة إلى إيجاد مخرج؛ ربما يكون هذا هو المخرج؛ لم يكن هناك ضرر من المحاولة. من ثم، طلب من ألكسندر أن يمضي قدما. إنها ستكون عملية ضخمة[4]، جهدا مشتركا من وكالة الأمن القومي، ووكالة الاستخبارات المركزية، والوحدة 8200، ومكتب الحرب السيبرانية في إسرائيل. في تلك الأثناء، استخدم ألكسندر خدعة بسيطة لبدء العملية. كان الإيرانيون ركّبوا أجهزة تسمى «مزودات الطاقة غير المنقطعة» Uninterruptible Power Supplies (UPS)[5] على المولدات التي كانت تمد مفاعل نطنز بالكهرباء، لمنع أنواع الطفرات (التموجات) أو الانخفاضات في الجهد الكهربائي التي من شأنها أن تلحق الضرر بأجهزة الطرد المركزي الدوارة. كان من السهل اختراق تلك المزودات. في أحد الأيام، حدثت طفرة وارتفع الجهد الكهربائي، ما أدى إلى انفجار خمسين من أجهزة الطرد المركزي. كانت تركيا هي التي أمدت إيران بمزودات الطاقة تلك؛ اشتبه الإيرانيون في أنه كان عملا تخريبيا، وتحولوا إلى مورد آخر ظنا

منهم أن هذا من شأنه أن يحل المشكلة. كان الإيرانيون على حق بشأن العمل التخريبي، ولكن ليس بشأن مصدره.

كان إيقاف تشغيل المفاعل عن طريق العبث بمصادر الإمداد بالطاقة خطوة لا تتكرر. بينما كان الإيرانيون يعملون على إصلاح المفاعل، أعدت وكالة الأمن القومي الجرعة المدمرة الأكثر ديمومة.

معظم هذا العمل أُنجز بواسطة صفوة مخترقي الحاسوب في «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو)، الذي كانت قدراته وموارده التقنية قد تعاظمت في أثناء العقد منذ أن خصص كين مينيهان أحد أركان مديرية استخبارات الإشارة (سيجينت) ليسمح لكادر جديد هو جماعة من العباقرة المهووسين بالحاسوب بأن يشعروا بالارتياح والاطمئنان ويعتادوا وضعهم الجديد. أما فيما يخص عملية «الألعاب الأولمبية»، فقد أخذوا بعضا من اختراعاتهم الأكثر جرأة - والتي أذهلت حتى أمهر محاربي استخبارات الإشارة القدامى الذين سمح لهم بالاطلاع على السر- ودمجوها معا في فيروس حاسوبي متنقل (دودة الحاسوب) واحد فائق أُطلق عليه اسم «لهب» Flame.

«لهب» Flame هو برمجية خبيثة متعددة الأغراض[6]، استوعبت 650 ألف سطر من التعليمات البرمجية (الكود) (أكبر من أي أداة اختراق نمطية بنحو 4 آلاف ضعف)، حالما يصيب «لهب» Flame أحد الحواسيب، كان يمكنه سرقة الملفات، ورصد الشاشات، وضغطات المفاتيح (ضربات المفاتيح)، وتشغيل ميكروفون الجهاز لتسجيل المحادثات الدائرة في الجوار، وتشغيل وظيفة «بلوتوث» Bluetooth الخاصة بالجهاز لسرقة البيانات من معظم الهواتف الذكية الموجودة في نطاق عشرين مترا، بالإضافة إلى حيل أخرى، كان كل ذلك يحدث من مراكز قيادة وكالة الأمن القومي في كل أرجاء العالم.

للولوج إلى عناصر التحكم (الضوابط)[7] في نطنز، طور مخترقو الحواسيب في «مكتب عمليات الولوج المصمم وفقا للحاجة» خمس أدوات برمجية للاستغلال الفوري من دون انتظار zero-day exploits لخمس ثغرات أمنية منفصلة لم يكن أحد قد اكتشفها من قبل في نظام التشغيل «ويندوز» Windows الخاص بوحدات التحكم التي أنتجتها شركة سيمنز Siemens. كان استغلال إحدى تلك الثغرات

الأمنية في الملف الخاص بلوحة المفاتيح يمنح «مكتب عمليات الولوج المصمم وفقا للحاجة» امتيازاتِ مستخدم استثنائية تسمح بالتحكم في كل وظائف الحاسوب. ثمة ثغرة أخرى كانت تتيح إمكانية الولوج إلى كل الحواسيب التي تتشارك معا إحدى الطابعات المصابة.

كانت الفكرة هي اختراق أجهزة سيمنز التي تتحكم في الصمامات التي تضخ غاز اليورانيوم إلى أجهزة الطرد المركزي. حالما يتحقق ذلك، كان «مكتب عمليات الولوج المصمم وفقا للحاجة» سيتلاعب بالصمامات، ويفتحها أكثر من اللازم، بما يفوق تحميل أجهزة الطرد المركزي، مما يؤدي إلى انفجارها.

استغرق الأمر ثمانية أشهر[8] لتعد وكالة الأمن القومي هذه الخطة وتصمم الفيروس الحاسوبي المتنقل (دودة الحاسوب) لتنفيذها. وكان ينبغي اختبار الفيروس الحاسوبي المتنقل. ابتدع كيث ألكسندر وروبرت غيتس تجربة، تضمن الجانب التقني لأجهزة الاستخبارات فيها بناء سلسلة متعاقبة من أجهزة الطرد المركزي مطابقة لتلك المستخدمة في نطنز، ووضعها في غرفة كبيرة في أحد مختبرات الأسلحة التابعة لوزارة الطاقة. كان التدريب مشابها لاختبار أورورا الذي جرى في الوقت نفسه تقريبا، والذي أثبت أنه كان من الممكن تدمير مولد كهربائي باستخدام وسائل سيبرانية بحتة. أسفرت تجربة محاكاة نطنز عن نتائج مماثلة، فقد وُجهت أجهزة الطرد المركزي لتدور بسرعة تبلغ خمسة أضعاف سرعتها العادية، حتى تحطمت إلى أشلاء. في الاجتماع التالي[9] بشأن هذا الموضوع في غرفة عمليات البيت الأبيض، وُضعت أنقاض أحد أجهزة الطرد المركزي تلك على الطاولة أمام الرئيس بوش. أعطى بوش الضوء الأخضر لإجراء التجربة على أرض الواقع.

كان هناك تحدٍ آخر[10]. بعد أن استبدل الإيرانيون مزودات الطاقة التركية التي خُربت، اتخذوا احتياطات إضافية لفصل حواسيب المفاعل عن الاتصال بالإنترنت. علم الإيرانيون بشأن أوجه الضعف والثغرات الأمنية في عناصر التحكم (الضوابط) الرقمية، وكانوا قد قرأوا أن تحويط الحواسيب بفجوة هوائية - عزلها عن الاتصال بالإنترنت، وجعل عملياتها التشغيلية مستقلة - كان أحد السبل للحد من الأخطار، إذ إن النظام إذا عمل على شبكة مغلقة، فلن يكون بإمكان قراصنة الحاسوب الولوج إليه، ومن ثم لن يكون في استطاعتهم إفساده، أو إضعافه، أو تدميره.

ما لم يكن الإيرانيون يعرفونه هو أن مخترقي الحواسيب في «مكتب عمليات الولوج المصمم وفقا للحاجة» كانوا منذ فترة طويلة قد اكتشفوا كيفية القفز فوق الفجوات الهوائية. أولا، كانوا قد نفذوا إلى شبكة بالقرب من الهدف المحيط بفجوة هوائية تحجبه عن الاتصال بالإنترنت، وبينما يبحرون في مساراتها، كانوا غالبا سيجدون وصلة ما أو بوابة ما، أغفلها مبرمجو أمن الحواسيب. إذا أدى ذلك المسار إلى طريق مسدود، فإنهم كانوا سيلجأون إلى شركائهم في مركز عمليات المعلومات التابع لوكالة الاستخبارات المركزية. قبل عقد من الزمان، في أثناء الحملة ضد الرئيس الصربي سلوبودان ميلوسيفيتش، تمكن جواسيس مركز عمليات المعلومات من الولوج إلى مبدلات الهاتف في بلغراد، وغرسوا أجهزة اخترقتها بعد ذلك فرق استخبارات الإشارة (سيجينت) التابعة لوكالة الأمن القومي، مما منحهم إمكانية الولوج إلى كامل نظام الهاتف بالبلاد. كانت مثل تلك الأنواع من العمليات المشتركة قد ازدهرت مع نمو وتطور «مكتب عمليات الولوج المصمم وفقا للحاجة».

أيضا، كانت وكالة الأمن القومي تتمتع بعلاقات وطيدة مع «الوحدة 8200» في إسرائيل، التي كانت لصيقة بجواسيس الموساد. إذا احتاج الأمر إلى الوصول إلى جهاز أو إلى شبكة مستقلة منغلقة غير موصولة بالإنترنت، فإن وكالة الأمن القومي كانت تستطيع اللجوء إلى أي من الجهات العديدة المتعاونة معها، مثل: مركز عمليات المعلومات، أو الوحدة 8200، أو دوائر التجسس المحلية، أو بعض مقاولي (متعهدي) الدفاع في عدد من الدول الحليفة، لغرس جهاز بث أو أداة إرشادية تنبيهية (بيكون) يستطيع «مكتب عمليات الولوج المصمم وفقا للحاجة» من خلالها تحديد موقعها والتوجه إليها.

في عملية «الألعاب الأولمبية»، كان أحدهم سيُثبّت البرمجية الخبيثة الضارة عن طريق إدخال ناقلة بيانات (وحدة ذاكرة فلاشية) في أحد الحواسيب (أو في طابعة يستخدمها عدد كبير من الحواسيب) في مقر المنشأة – تقريبا بالأسلوب ذاته الذي كان جنود السيبرانية الروس يستخدمونه - في الوقت نفسه تقريبا - لاختراق الشبكات السرية للقيادة المركزية للولايات المتحدة في أفغانستان، ذلك التسلل الذي اكتشفته وكالة الأمن القومي وصدته في عملية «اليانكي صائد الظباء» (Buckshot Yankee).

لم تكن البرمجيات الخبيثة[11] ستسيطر على صمامات مضخات مفاعل نطنز فقط، بل كانت أيضا ستحجب تدخل المشرفين على المفاعل. على نحو اعتيادي، كانت عناصر التحكم (الضوابط) في الصمام ستطلق تنبيها حينما يتسارع تدفق اليورانيوم بوتيرة سريعة. لكن البرمجية الخبيثة سمحت لـ «مكتب عمليات الولوج المصمم وفقا للحاجة» باعتراض التنبيه واستبداله بإشارة مزيفة كاذبة، تشير إلى أن كل شيء على ما يرام.

كان من الممكن تصميم الفيروس الحاسوبي المتنقل (دودة الحاسوب) لتدمير كل أجهزة الطرد المركزي، لكن هذا كان سيثير الشكوك في أنها عملية تخريب. اكتشف مهندسو العملية مسارا أفضل، وهو الإضرار بعدد من أجهزة الطرد المركزي بما يكفي فقط لجعل الإيرانيين يَعزون سبب الإخفاق إلى الخطأ البشري، أو إلى سوء التصميم. بعد ذلك كانوا سيفصلون العلماء المثاليين والملائمين تماما، ويستبدلون المعدات الجيدة والملائمة تماما، مما يعرقل برنامجهم النووي بدرجة أكبر.

وبهذا المفهوم، كانت عملية «الألعاب الأولمبية» هي حملة كلاسيكية نموذجية لوسائل حرب المعلومات، إذ لم يكن الهدف هو البرنامج النووي الإيراني فقط، ولكن أيضا ثقة الإيرانيين في مستشعراتهم، ومعداتهم، وفي أنفسهم.

كانت الخطة جاهزة للانطلاق، لكن مدة جورج بوش في المنصب أشرفت على الانتهاء. كان الأمر سيعود إلى باراك أوباما.

بالنسبة إلى بوش لم تكن الخطة في حاجة إلى تفكير، تماما مثل خطة إرسال رسائل بريد إلكتروني مزيفة كاذبة إلى المتمردين العراقيين. إنها كانت أيضا منطقية في نظر أوباما. منذ مستهل رئاسته، أفصح أوباما عن فلسفة بشأن استخدام القوة، وكان غالبا يتبعها، إنه كان على استعداد للقيام بعمل عسكري، إذا كانت المصالح القومية تتطلب ذلك، وإذا كانت الأخطار محدودة جدا؛ لكن ما لم تكن المصالح الحيوية الأساسية على المحك، فإنه كان يعزف عن إرسال آلاف من القوات الأمريكية، لا سيما بالنظر إلى هدر واستنزاف الحربين اللتين ورثهما في أفغانستان والعراق. كان البرنامجان السريان اللذان ضغط عليه بوش للاستمرار فيهما – ضربات الطائرات المسيَّرة من دون طيار ضد الجهاديين، والتخريب السيبراني لمحطة تخصيب اليورانيوم في إيران - يناسبان منطقة ارتياح أوباما، إذ إن كليهما كان يخدم مصلحة قومية، ولا يخاطر بحياة الأمريكيين.

حالما وصل أوباما إلى البيت الأبيض[12]، أعرب عن بضعة هواجس بشأن الخطة، إذ كان يرغب في ضمانات بأنه حينما يصيب الفيروس الحاسوبي المتنقل مفاعل نطنز، فإنه لن يسبب أيضا انطفاء الأنوار في محطات الطاقة، أو المستشفيات، أو المرافق المدنية الأخرى المجاورة.

سلم وأقر من كانوا يطلعونه على الخطة بأن الفيروسات الحاسوبية المتنقلة كان يمكن أن تنتشر، ولكن هذا الفيروس الحاسوبي المتنقل على وجه الخصوص كان مبرمجا[13] للبحث عن برمجية «سيمنز» بعينها؛ وإذا انجرف عن مساره إلى مناطق بعيدة، ولم تكن البرمجية المعنية موجودة لدى الأهداف العفوية غير المقصودة، فهو لم يكن ليلحق بها أي ضرر.

كان أوباما قد أبقى على غيتس، وبالفعل كان له تأثير كبير في تفكيره، وكان يشجع الرئيس الجديد على تجديد الضوء الأخضر للاستمرار في العملية. لم يكن أوباما يرى أي مبرر لعدم القيام بذلك.

بعد مضي أقل من شهر على تولي أوباما منصبه، كان الفيروس الحاسوبي المتنقل قد حقق نجاحه الأول، فقد خرجت سلسلة من أجهزة الطرد المركزي في نطنز عن نطاق السيطرة، وتحطم الكثير منها. اتصل أوباما هاتفيا ببوش ليخبره[14] بأن البرنامج السري الذي ناقشاه معا كان يحقق إنجازا.

في شهر مارس، غيّرت وكالة الأمن القومي من نهجها[15]. في المرحلة الأولى، اخترقت العملية الصمامات التي تتحكم في معدل تدفق غاز اليورانيوم إلى أجهزة الطرد المركزي. في المرحلة الثانية، كان الهجوم يسعى إلى الأجهزة المعروفة باسم «محولات التردد» (frequency converters)، التي تتحكم في سرعة دوران أجهزة الطرد المركزي. كانت السرعة العادية[16] تتراوح بين نحو 800 و1200 دورة في الثانية، وتمكن الفيروس الحاسوبي المتنقل من تسريعها تدريجيا حتى تصل إلى 1410 دورات، النقطة التي عندها تحطمت عدة أجهزة للطرد المركزي إلى أشلاء طارت في الهواء. في بعض الأحيان، كانت تبطئ المحولات فترة تبلغ أسابيع عدة، إلى ما لا يتجاوز دورتين في الثانية؛ نتيجة لذلك، لا يتمكن غاز اليورانيوم من الخروج من جهاز الطرد المركزي سريعا بما يكفي. سيؤدي عدم التوازن إلى حدوث اهتزازات كانت ستسبب ضررا شديدا لأجهزة الطرد المركزي بطريقة مختلفة.

بغض النظر عن الأسلوب، كان الفيروس الحاسوبي المتنقل يغذي أيضا شاشات رصد النظام ببيانات كاذبة خاطئة، إلى درجة أن كل شيء كان يبدو طبيعيا للعلماء الإيرانيين الذين كانوا يراقبونها. وعندما ضربتهم الكارثة، لم يدركوا ما الذي كان قد حدث. إنهم كانوا قد عانوا مشكلات تقنية[17] في أجهزة الطرد المركزي منذ بداية البرنامج؛ بدا الأمر مثل مزيد من الشيء نفسه، ولكن أشد وأعنف، ومزيد من الاضطرابات المتكررة. وكانت وكالة الأمن القومي قد صممت الفيروس الحاسوبي المتنقل (دودة الحاسوب) لجعل الأمور تبدو كذلك.

مع بداية العام 2010[18]، فإن نحو ربع أجهزة الطرد المركزي الإيرانية – نحو ألفين من أصل 8700 جهاز طرد مركزي - كان قد أصابه عطب إلى حد لا يمكن إصلاحه. قدر محللو استخبارات الولايات المتحدة حدوث انتكاس في برنامج التخصيب النووي الإيراني وتعطل لمدة تتراوح بين عامين وثلاثة أعوام.

بعد ذلك، في بدايات ذلك الصيف، ساءت الأمور. الرئيس أوباما، الذي كان قد اطلع[19] على كل التفاصيل وأُبلغ بكل نجاح أو إخفاق، أخبره مستشاروه بأن الفيروس الحاسوبي المتنقل خرج عن السيطرة، إذ إنه، لأسباب غير واضحة كليا، كان قد قفز من حاسوب إلى آخر، وشق طريقه إلى خارج شبكة نطنز، ثم إلى شبكة أخرى أبعد من ذلك. لم يكن سيسبب أي ضرر - مثلما كان قد أخبره من أطلعوه من قبل، إذ بُرمج لإيقاف تشغيله إذا لم يجد وحدة تحكم سيمنز معينة - لكن كان وجوده سينكشف، وكان الإيرانيون سيكتشفون في نهاية المطاف ما الذي كان يجري. كانت عملية «الألعاب الأولمبية» على شفا أن تكون في مهب الريح.

في آن واحد تقريبا[20]، بدأت بعض كبريات شركات أمن البرمجيات في العالم، مثل: «سيمانتيك» Symantec في كاليفورنيا، و«فيروس بلوك أدا» VirusBlokAda في بيلاروسيا، و«مختبر كاسبارسكي» Kaspersky Lab في روسيا، ترصد فيروسا غريبا آخذا في الظهور حول العالم بصورة عشوائية. في البداية، لم يعرفوا منشأه أو الغرض منه، ولكن بعد تقصي جذوره، والتحليل اللغوي لتعليماته البرمجية (الكود)، وقياس حجمه، أدركوا أنهم توصلوا إلى أحد الفيروسات الحاسوبية المتنقلة المدروسة بعناية، والأكثر تطورا وتفصيلا على مر التاريخ. أصدرت شركة مايكروسوفت Microsoft تقريرا إرشاديا[21] لعملائها، وشكلت جناسا من الأحرف القليلة الأولى في التعليمات

البرمجية للفيروسات الحاسوبي المتنقل، وأطلقوا على الفيروس الحاسوبي اسم «ستوكسنت» Stuxnet - وهو الاسم الذي اشتهر به.

بحلول شهر أغسطس كانت شركة «سيمانتيك» Symantec قد كشفت[22] عن أدلة كافية لإصدار بيان خاص بها، محذرة من أن «ستوكسنت» لم يُصمم بغرض الاختراق العابث أو حتى للتجسس، بل بالأحرى للتخريب. في سبتمبر، استشف باحث ألماني متخصص في الأمن[23] يدعى رالف لانغنر Ralph Langner، استشف من الحقائق المتاحة أن شخصا ما كان يحاول تعطيل مفاعل نطنز النووي في إيران، وربما كان الإسرائيليون متورطين في هذا.

عند هذه النقطة أصاب الهلع بعض مخبري البرمجيات الأمريكيين[24]: هل هم من فورهم كانوا قد ساعدوا على فضح عملية سرية جدا لاستخبارات الولايات المتحدة؟ لم يكن في مقدورهم أن يعرفوا ذلك حينئذ، ولكن فضولهم والتزامهم المهني نحو توعية الجمهور بشأن فيروس حاسوب طليق وربما يكون ضارا، كان لهما ذلك التأثير. بعد وقت قصير من بيان شركة سيمانتيك Symantec، حتى قبل تكهن لانغنر العلمي البارع بشأن الهدف الحقيقي لفيروس «ستوكسنت»، استخلص الإيرانيون الاستدلال المناسب (لذلك كان هذا إذن هو السبب في خروج أجهزة الطرد المركزي عن السيطرة) وقطعوا كل الروابط بين محطة نطنز ووحدات تحكم سيمنز.

علم أوباما بالانكشاف في أثناء اجتماع في البيت الأبيض[25]، حينئذ سأل كبار مستشاريه عما إذا كان يتعين عليهم إنهاء العملية. قيل له إنها مازالت تسبب أضرارا، على رغم ما اتخذه الإيرانيون من تدابير مضادة؛ أمر أوباما وكالة الأمن القومي بأن تعمل على تكثيف البرنامج وإصابة أجهزة الطرد المركزي بتشويهات أعنف؛ وتسريعها ثم إبطائها، من دون أي اهتمام بشأن الكشف، لأن غطاءها قد سقط بالفعل.

أوضح تقييم الموقف[26] أنه في الأسابيع التالية للانكشاف، أُخرج ألف جهاز طرد مركزي أخرى من العمل من أصل 5 آلاف جهاز كانت متبقية.

حتى بعد انتهاء عملية «الألعاب الأولمبية»، فإن فن وعلم مهاجمة شبكة الحاسوب (سي إن أيه) دُفع به قُدما. في الواقع بحلول نهاية أكتوبر، حينما أصبحت

القيادة السيبرانية للولايات المتحدة على أتم الاستعداد للعمليات، برز «هجوم شبكات الحاسوب» باعتباره نشاطا نهما مستنزفا، بل حتى متسلطا ومهيمنا على فورت ميد.

قبل ذلك بعام، واستباقا لتوجيه روبرت غيتس باستحداث القيادة السيبرانية، أصدر رئيس الهيئة المشتركة لرؤساء الأركان، الجنرال بيتر بيس، وثيقة سرية هي «الاستراتيجية العسكرية القومية للعمليات السيبرانية» (National Military Strategy for Cyber Operations)، التي أعربت عن الحاجة إلى «قدرات هجومية في الفضاء السيبراني[27] لاكتساب القدرة على المبادأة والحفاظ عليها».

وبعد أن صار الجنرال ألكسندر قائد القيادة السيبرانية وكذلك مدير وكالة الأمن القومي، كان يُجهز أربعين «فريقا للهجوم السيبراني»[28] - سبعة وعشرين لقيادات الولايات المتحدة المقاتلة (القيادة المركزية، وقيادة الباسيفيك - المحيط الهادئ -، والقيادة الأوروبية، وما إلى ذلك)، وثلاثة عشر تضطلع بحماية الشبكات داخل البلاد، بصفة رئيسية شبكات وزارة الدفاع. وكان جزء من هذه المهمة الأخيرة يتضمن رصد الشبكات. بفضل ما أُنجز من عمل خلال العقد السابق، بدءا من مركز سلاح الجو لوسائل حرب المعلومات، ثم التوسع التدريجي إلى الفروع العسكرية الأخرى، كان لدى الشبكات العسكرية القليل جدا من نقاط الوصول إلى الإنترنت – كانت في ذلك الوقت عشرون نقطة فقط، ثم خُفّضت إلى ثماني نقاط في خلال الأعوام القليلة اللاحقة – التي كان في مقدور فرق ألكسندر استطلاعها وصد الهجمات التي تأتي فجأة عبر أبواب خلفية. لكن حماية الشبكات كانت تعني أيضا الهجوم، من خلال مفهوم «استغلال شبكة الحاسوب» (سي إن إي) المبهم عمدا، والذي كان يمكن أن يكون شكلا من أشكال «الدفاع الإيجابي»، وكذلك التجهيز لـ «مهاجمة شبكة الحاسوب» (سي إن أيه).

بعض المسؤولين في عمق مؤسسة الأمن القومي انتابهم القلق من هذا الاتجاه. كان الجيش - الأمة - على نحو سريع يتبنى شكلا جديدا لوسائل الحرب، كان قد حشد واستخدم نوعا جديدا من الأسلحة، لكن كل هذا كان يتم في غاية السرية، داخل وكالة الاستخبارات الأكثر تكتما في البلاد، وكان جليا، حتى بالنسبة إلى أولئك الذين لديهم لمحة غير واضحة عن أعمال الوكالة الداخلية، أنه لم يكن

أحد قد فكر مليا في تداعيات هذا النوع الجديد من الأسلحة، وهذه الرؤية الجديدة للحرب.

في أثناء التخطيط لعملية «ستوكسنت»، كان هناك جدال داخل إدارة كل من بوش وأوباما، بشأن السبق الذي ربما يؤسسه الهجوم. على مدار أكثر من عَقد من الزمان، كانت عشرات الفرق الاستشارية واللجان قد حذّرت من أن البنية الأساسية الحرجة الأمريكية عرضة لهجوم سيبراني، والآن كانت أمريكا تطلق أول هجوم سيبراني على البنية الأساسية الحرجة لدولة أخرى. تقريبا لم يكن أحد يعارض صراحة على نحو قاطع برنامج ستوكسنت، لأنه إذا كان في إمكانه منع إيران من تطوير أسلحة نووية، فإن الأمر يستحق المخاطرة. لكن كان كثير من المسؤولين يدركون أنها كانت مخاطرة، وأن الأخطار المترتبة على ردة الفعل كانت محتومة وهائلة.

في نهاية المطاف، لم تكن الولايات المتحدة وحدها على متن هذه المركبة الفضائية السيبرانية. لقد كان الروس يعززون ويكثفون قدراتهم على استغلال شبكات الحاسوب ومهاجمتها، منذ أن نفذوا إلى مواقع وزارة الدفاع قبل عقد من الزمان، في عملية «متاهة ضوء القمر». كان الصينيون قد انضموا إلى الركب في العام 2001، وسرعان ما صاروا بارعين في النفاذ إلى الشبكات الحساسة التي تخص العشرات من القيادات العسكرية، والمرافق، والمختبرات الأمريكية (على الرغم من ذلك، وكما يعرف الجميع، فهي غير سرية). في أثناء العام الأول من فترة رئاسة أوباما[29]، نحو يوم الرابع من يوليو، «يوم الاستقلال»، شنت كوريا الشمالية (التي كان مواطنوها يحصلون على الكهرباء بصعوبة) هجوما هائلا لحجب الخدمة، أدى إلى إغلاق مواقع الويب الخاصة بوزارة الأمن الداخلي، ووزارة الخزانة، ووزارة النقل، والخدمة السرية، ولجنة التجارة الفدرالية، وبورصة نيويورك، وبورصة «ناسداك» NASDAQ، بالإضافة إلى العشرات من بنوك كوريا الجنوبية، ما أثر فيما لا يقل عن 60 ألفا، وربما ما يصل إلى 160 ألف حاسوب.

استحثت عملية ستوكسنت الإيرانيين على استحداث وحدة حرب سيبرانية خاصة بهم، وقد انطلقت إلى مستويات تمويلية أعلى خلال فترة العام ونصف العام اللاحقة[30]. في ربيع العام 2012، في هجوم تكميلي، حينما محا فيروس اللهب Flame الخاص بوكالة الأمن القومي - البرمجية الخبيثة الهائلة، والمتعددة الأغراض التي اعتمدت عليها عملية «الألعاب الأوليمبية» - معظم محتويات محركات

الأقراص الصلبة في وزارة النفط الإيرانية، وفي شركة النفط الوطنية الإيرانية. بعد مضي أربعة أشهر[31]، ردت «إيران» الهجوم بفيروس «شمعون» Shamoon الخاص بها، إذ محا محتويات 30 ألف محرك أقراص صلبة (عمليا، كل محرك أقراص صلبة في كل محطة عمل workstation) في شركة أرامكو السعودية، شركة النفط المشتركة بين الولايات المتحدة والمملكة العربية السعودية، وغرس على شاشات الحواسيب في جميع محطات العمل، صورة العلم الأمريكي وهو يحترق.

من خلال اعتراض الاتصالات، علم كيث ألكسندر أن الإيرانيين طوروا وأطلقوا «شمعون» خصيصا بغرض القصاص، وليكون ردا على عمليتي ستوكسنت واللهب. كان ألكسندر في طريقه إلى مؤتمر مع «مقر الاتصالات الحكومية» (جي سي إتش كيو)، الصنو البريطاني لوكالة الأمن القومي، وكان يطالع مذكرة بشأن نقاط الحوار كتبها أحد معاونيه، مشيرا إلى أنه مع شمعون وكثير من الهجمات السيبرانية الأخيرة على البنوك الغربية، فإن الإيرانيين كانوا قد «أظهروا مقدرة واضحة[32] على التعلم من قدرات وأفعال الآخرين»، تحديدا، قدرات وأفعال وكالة الأمن القومي والوحدة 8200 في إسرائيل.

كان هذا هو أحدث تجسيد مأساوي مثير لما كان قد توقعه محللو ومديرو الوكالة طوال عقود من الزمان، الشيء الذي يمكننا فعله بهم، فإنهم يوما ما يمكنهم أن يفعلوه بنا، فيما عدا أن «يوما ما» صار الآن.

تزامنت فترة ألكسندر بوصفه مديرا لوكالة الأمن القومي ليس فقط مع تقدم الأسلحة السيبرانية وبداية الهجمات السيبرانية الفتاكة المخربة ماديا، بل أيضا مع بداية تصاعد سباق التسلح السيبراني، وقد كان ألكسندر ذاته يشجع ذلك ويتبناه. ما الذي ينبغي فعله حيال ذلك؟ كان هذا أيضا سؤالا لم يكن أحد قد فكر فيه، ولا حتى على أدنى المستويات.

في السابق، في نهاية العام 2006، حينما صار «بوب غيتس» وزيرا للدفاع، كان مدهوشا جدا من حجم محاولات التسلل إلى الشبكات العسكرية الأمريكية. كانت الإحاطات التي تعرض عليه تشتمل على قوائم تعدد العشرات، وأحيانا المئات، كل يوم؛ حتى إنه كان قد كتب مذكرة إلى نائب المستشار القانوني للبنتاغون سأل فيها: عند أي نقطة[33] تكون إحدى الهجمات السيبرانية بمنزلة عمل من أعمال الحرب بموجب القانون الدولي؟

لم يتلق غيتس ردا حتى اليوم الأخير من العام 2008، بعد مضي نحو عامين. كتب المستشار القانوني للبنتاغون: نعم، ربما يرقى الهجوم السيبراني إلى المستوى الذي يستدعي ردا عسكريا، كان يمكن اعتباره عملا من أعمال العدوان المسلح في ضوء ظروف معينة، ولكن ما تلك الظروف، وأين ينبغي أن يكون الحد الفاصل، بل وحتى معايير رسم هذا الحد الفاصل؟ كانت مسائل يتصدى لها صانعو السياسة، لا المحامون. أخذ غيتس الرد على أنه مراوغة وتملص، وليس إجابة.

كانت إحدى العقبات التي تحول دون الحصول على إجابة أكثر وضوحا - وتفكير بصفاء أكثر، بوجه عام - هي أن كل شيء بشأن الحرب السيبرانية كان يكتنفه الغموض ومحاطا بالسرية، فقد غُرست جذورها، ونضجت ثمارها وجُنيت، في وكالة كان وجودها ونشأتها من الأساس غاية في السرية، ومع ذلك كانت عملياتها تجري بدقة، وعلى نحو محكم مثل أي من دوائر الحكومة.

في السابق، كان لثقافة السرية التامة هذه سبب منطقي محدد، وقتما كانت استخبارات الإشارة أداة استخباراتية بحتة، حينما كان السر الكبير هو أن وكالة الأمن القومي كانت قد كسرت شفرة أحد الخصوم؛ إذا كُشِف عن ذلك، كان الخصم سيغير الشفرة ببساطة؛ حينئذ كان سيتعين على الوكالة أن تبدأ من جديد، وإلى أن تنجح في حل الشفرة الجديدة، كان من الممكن أن يتضرر الأمن القومي؛ وفي زمن الحرب، ربما نخسر إحدى المعارك.

لكن حاليا، بعد أن صار مدير وكالة الأمن القومي هو أيضا قائدا من فئة النجمات الأربع، وبعد أن أُقحمت استخبارات الإشارة في سلاح للدمار، ما يشبه قنبلة يتم التحكم فيها من بُعد، برزت تساؤلات وجرت مجادلات، بشأن الاعتبارات ذات العلاقة، ليس فقط بالمبادئ الأخلاقية للسلاح الجديد، ولكن بفائدته وجدواه الاستراتيجية - تحديد آثاره، وآثاره الجانبية، وعواقبه على وجه الدقة.

كان الجنرال «مايكل هايدن»، المدير السابق لوكالة الأمن القومي، قد انتقل إلى «لانغلي» بوصفه مديرا لوكالة الاستخبارات المركزية، حينما أعطى الرئيس بوش الضوء الأخضر لعملية «الألعاب الأولمبية» (أُزيح من ذلك المنصب حينما جاء أوباما إلى البيت الأبيض، لذلك لم يكن لـ هايدن دور في العملية الفعلية). بعد عامين من انهيار عملية ستوكسنت ووصولها إلى طريق مسدود، حينما

تسربت تفاصيل بشأنها إلى الصحافة الرئيسية، أعرب هايدن - هو الآن متقاعد من الجيش - علنا عن المخاوف ذاتها التي كان قد تجادل بشأنها هو وآخرون في غرفة العمليات بالبيت الأبيض.

قال هايدن لأحد المراسلين: «كان للهجمات السيبرانية السابقة تأثير[34] محدود في الحواسيب الأخرى. هذا هو الهجوم الأول الذي له سمة رئيسية هي استخدام هجوم سيبراني لإحداث تأثير تدميري مادي. وبغض النظر عما تعنيه التأثيرات لك - وأنا أعتقد أن تدمير سلسلة متتالية من أجهزة الطرد المركزي الإيرانية أمر حسن لا تشوبه شائبة - فلا يمكنك إلا أن تصفه بأنه هجوم على البنية الأساسية الحرجة».

واستطرد هايدن: «شخص ما قد عبر روبيكون(*). أصبح لدينا الآن فيلق على الجانب الآخر من النهر»، شيء ما كان قد تغير في طبيعة وسائل الحرب وحساباتها، تماما مثلما حدث بعد أن كانت الولايات المتحدة قد ألقت قنابل ذرية على «هيروشيما» Hiroshima و«ناغازاكي» Nagasaki في نهاية الحرب العالمية الثانية. قال هايدن: «لا أريد الادعاء أن لها تأثيرا مماثلا، ولكن على الأقل إلى حد ما، إنه أغسطس من العام 1945».

طوال أول عقدين من الزمان، بعد «هيروشيما»، كانت الولايات المتحدة تتمتع بتفوق كمي هائل - ولبعض من ذلك الوقت، احتكار - في الأسلحة النووية. لكن على مشارف حقبة جديدة في الحرب السيبرانية، كانت الحقيقة المعروفة هي أن معظم الدول الأخرى كانت لديها وحدات حرب سيبرانية، وكانت أمريكا عرضة لخطر هذا النوع من الحرب أكثر من أي خصم محتمل، أكثر من أي دولة أخرى على ظهر هذا الكوكب، لأنها على نحو كثيف جدا تعتمد على شبكات الحاسوب غير الحصينة، في أنظمة أسلحتها، وأنظمتها المالية، وبنيتها الأساسية الحرجة الحيوية.

(*) روبيكون Rubicon: هو نهر في شمال إيطاليا، يجري بطول 24 كيلومترا، ويصب في البحر الأدرياتيكي. يعود الاسم إلى الكلمة اللاتينية rubicundus التي تعني أحمر، إشارة إلى لون التربة على ضفافه. في أزمنة قديمة، كان نهر روبيكون جزءا من الحدود بين إيطاليا الرومانية و«جاليا كيسالبينا» Gallia Cisalpina، أو بلاد الغال، وهو إقليم قديم في شمال إيطاليا، يقع شمال إقليمي «ليغوريا» Liguria و«أومبريا» Umbria وجنوب الألب، وكان أهله في نزاع دائم مع روما. يعود الفضل في شهرة نهر روبيكون إلى يوليوس قيصر، كان محظورا على يوليوس قيصر العبور بجنوده خارج حدود الإقليم الذي أرسلوا إليه، لكنه عبر النهر مخالفا لأوامر قادته في روما في مجلس الشيوخ (سيناتوس) Senatus، من ثم اندلعت حرب أهلية. وقد أصبح عبور نهر روبيكون تعبيرا سياسيا ذائع الصيت يستخدم للإشارة إلى الوصول إلى «نقطة اللاعودة». [المترجم].

إذا أرادت أمريكا، أو القيادة السيبرانية للولايات المتحدة، شن حرب سيبرانية، فإنها كانت ستقوم بذلك من داخل بيت زجاجي.

كان هناك اختلاف آخر بين هذين النوعين من الأسلحة الجديدة، إلى جانب حجم الأضرار التي كان يمكن أن تنزلها. كانت الأسلحة النووية موجودة في العلن، جوانب معينة بشأن إنتاجها أو حجم مخزونها هي التي كانت على وجه الدقة مصنفة على أنها سرية، لكن الجميع كان يعرف من الذي كانت لديه هذه الأسلحة، الجميع كان قد شاهد الصور ومقاطع الأفلام التي تبين ما الذي كان يمكن أن تفعله هذه الأسلحة إذا استُخدمت؛ وفي حالة ما إذا استُخدمت، كان الجميع سيعرف من الذي أطلقها.

كانت الأسلحة السيبرانية - وجودها، واستخدامها، والسياسات المحيطة بها - لاتزال مصنفة على أنها سرية. وبدا أن الولايات المتحدة وإسرائيل خربتا مفاعل «نطنز» (ناتنز)، وأن إيران محت محتويات محركات الأقراص الصلبة الخاصة بأرامكو السعودية، وأن كوريا الشمالية شنت هجمات حجب الخدمة على مواقع ويب الولايات المتحدة والبنوك في كوريا الجنوبية؛ لكن لم يُدن أي أحد في تلك الاعتداءات. وبينما كان خبراء التحليل الجنائي الذين كانوا يتعقبون الهجمات واثقين بتقييماتهم، فإنهم لم يتباهوا - لم يكن في استطاعتهم ذلك - بوصفه اليقين الذي لا يمكن دحضه، والذي يكون لدى فيزيائي يتعقب قوس مسار إحدى القذائف التسيارية (الصواريخ الباليستية).

اتسع هذا التكتم المفرط الصارم لا ليشمل عامة الجماهير فقط، لكنه انتشر أيضا داخل الحكومة، حتى بين معظم المسؤولين الرسميين من ذوي الصلاحيات الأمنية عالية المستوى. في السابق، في مايو من العام 2007، فإن مايك ماكونيل الذي صار بعد ذلك مديرا للاستخبارات القومية. وبعد فترة وجيزة من إطلاع جورج دبليو بوش على خطة إطلاق الهجمات السيبرانية ضد المتمردين العراقيين. أبرم اتفاقا مع كبار المسؤولين الرسميين في البنتاغون، ووكالة الأمن القومي، ووكالة الاستخبارات المركزية، ومكتب المدعي العام؛ اتفاقا بعنوان «مذكرة اتفاق ثلاثية الأطراف[35] فيما بين وزارة الدفاع، ووزارة العدل، وأجهزة الاستخبارات بشأن أنشطة مهاجمة شبكة الحاسوب واستغلال شبكة الحاسوب». لكن بغض النظر عن شرطٍ مفاده أن

العمليات الهجومية السيبرانية تتطلب موافقة رئاسية، لم تكن هناك إجراءات أو بروتوكولات رسمية (إجراءات نظامية) يتبعها كبار المستشارين السياسيين وصناع القرار لتقييم أهداف، أو أخطار، أو فوائد، أو عواقب مثل هذه الهجمات.

لملء هذا الفراغ الشاسع، أمر الرئيس أوباما بإعداد مسودة توجيه رئاسي جديد متعلق بالسياسات، «بي بي دي - 20» (PPD-20)، بعنوان «سياسة العمليات السيبرانية بالولايات المتحدة»، وقد وقعه في أكتوبر من العام 2012، بعد بضعة أشهر من أول تسريبات صحافية ضخمة بشأن ستوكسنت.

كان ذلك التوجيه، الذي جاء في ثماني عشرة صفحة، هو الأكثر صراحة وتفصيلا. من ناحية، كان نهجه أكثر حذرا وحيطة مما سبقه من توجيهات؛ على سبيل المثال، وفي إشارة ضمنية (لكن غير معلنة) إلى انكشاف ستوكسنت، ذكر التوجيه أنه يمكن أن تنتشر آثار هجوم سيبراني إلى «مواقع أخرى غير المواقع المستهدفة، مع احتمال حدوث تداعيات وآثار عفوية غير مقصودة أو جانبية، والتي ربما يكون لها أثر في المصالح القومية للولايات المتحدة». أسس التوجيه الرئاسي مجموعة عمل مشتركة بين الوكالات تضطلع بسياسات العمليات السيبرانية لضمان إمكان تدبر مثل تلك الآثار الجانبية - إلى جانب قضايا السياسة العامة الأخرى - وتقييمها قبل ابتداء إحدى الهجمات.

لكن المقصد والأثر الرئيسي الأهم للتوجيه الرئاسي «بي بي دي - 20» كان إضفاء الطابع المؤسسي على الهجمات السيبرانية باعتبارها أداة تكاملية مكملة للدبلوماسية والحرب الأمريكية، ولا تتجزأ عنها. نص التوجيه الرئاسي على أن الوزارات والدوائر ذات الصلة «ستحدد الأهداف المحتملة ذات الأهمية القومية» التي في مواجهتها «يمكن أن تقدم الهجمات السيبرانية توازنا ملائما بين الفعالية والأخطار مقارنة بغيرها من أدوات السلطة القومية». على وجه التحديد، فإن وزير الدفاع، ومدير الاستخبارات القومية، ومدير وكالة الاستخبارات المركزية، بالتنسيق مع المدعي العام، ووزير الخارجية، ووزير الأمن الداخلي، ورؤساء دوائر الاستخبارات ذات الصلة «سيعدون خطة يقرها الرئيس... تحدد ما هو متوقع من أنظمة، وإجراءات، وبنية أساسية على أساسها كان يتعين على الولايات المتحدة أن تكرس، وتتذرع بقدرات [سيبرانية هجومية]؛ ويقترح الظروف التي في ضوئها يمكن

استخدام [تلك القدرات]؛ ويقترحون الموارد وخطوات الاستعداد الضرورية التي كانت ستلزم للتنفيذ، والتنقيح، والتحديث، بما يتوافق مع تغير احتياجات الأمن القومي للولايات المتحدة».

كان من المقرر تحليل الخيارات السيبرانية باستمرار وعلى نحو منهجي، والتخطيط المسبق لها، ودمجها في الخطط الحربية الأشمل، بالطريقة ذاتها التي قد كانت متبعة للخيارات النووية في أثناء الحرب الباردة.

كذلك، وكما هي الحال مع الخيارات النووية، فإن التوجيه كان يطلب «موافقة رئاسية خاصة» لأي عملية سيبرانية كانت تعتبر أنها «من المرجح على نحو معقول أن تسفر عن عواقب وآثار جسيمة يعتد بها»، هاتان الكلمتان الأخيرتان محددتان لتتضمنا «خسارة في الأرواح، أو ردود أفعال جسيمة ضد الولايات المتحدة يعتد بها، أو أضرارا جسيمة بالممتلكات يعتد بها، أو عواقب وخيمة خطرة في السياسة الخارجية للولايات المتحدة، أو أثرا اقتصاديا خطرا على الولايات المتحدة»، على الرغم من وجود استثناء مفاده السماح لمدير دائرة ذات صلة، أو وزير في وزارة معنية، بإطلاق هجوم في حالة الطوارئ من دون الحصول على موافقة رئاسية.

على الرغم من ذلك، خلافا للخيارات النووية، لم يقصد أن تبقى خطط العمليات السيبرانية خاملة ساكنة إلى أن يبلغ النزاع منتهاه؛ كان من المفترض أن تُنفَّذ، وعلى نحو متكرر إلى حد ما. نص التوجيه على أن رؤساء الدوائر والوزراء الذين يديرون تلك الهجمات «سيقدمون إلى الرئيس، من خلال مستشار الأمن القومي، تقارير سنوية بشأن استخدام عمليات العام السابق وفعاليتها».

لم يُهدَر وقتٌ لإعداد وتجهيز الخطط. أشار أحد تقارير العمل بشأن التوجيه[36] إلى أن وزير الدفاع، ومدير الاستخبارات القومية، ومدير الاستخبارات المركزية قدموا إحاطة بشأن خططهم في اجتماع محدود لنواب مجلس الأمن القومي، في شهر أبريل من العام 2013، بعد ستة أشهر من توقيع التوجيه الرئاسي المتعلق بالسياسات «بي بي دي - 20».

كان التوجيه الرئاسي المتعلق بالسياسات «بي بي دي - 20» مصنفا على أنه سري جدا، ولا يمكن تشاركه مع المسؤولين الرسميين الأجانب. وجود الوثيقة في حد ذاته كان غاية في السرية، لكنها كانت موجهة إلى رؤساء كل الدوائر والوزارات المعنية،

وإلى نائب الرئيس، وكبار مساعدي البيت الأبيض. بعبارة أخرى، كان الموضوع يُناقَش، ليس فقط في تلك الدوائر النخبوية، ولكن أيضا - مع انكشاف ستوكسنت - بين العامة. بحذر شديد، بدأ المسؤولون يعترفون، بعبارات عامة وفضفاضة، بوجود العمليات الهجومية السيبرانية وبمفهومها.

الجنرال «جيمس كارترايت» James Cartwright الذي كان قد تقاعد أخيرا من منصب نائب رئيس الهيئة المشتركة لرؤساء الأركان، والذي كان قبل ذلك رئيسا للقيادة الاستراتيجية للولايات المتحدة التي كانت لها رقابة اعتبارية على العمليات السيبرانية، أخبر مراسلا صحافيا يغطي عملية ستوكسنت أن التكتم المفرط المغالى فيه الذي يحيط بالموضوع أضر بالمصالح الأمريكية. قال كارترايت: «لا يمكن أن يكون لديك شيء سري[37] ويكون رادعا، لأنك إذا لم تكن تعلم بوجوده، فإنه لن يخيفك».

رفض بعض الضباط منطق كارترايت، إذ إن الروس والصينيين كانوا يعرفون ما الذي كان لدينا، تماما مثلما كنا نعرف ما الذي كان لديهم. ومع ذلك، اتفق آخرون على أنه ربما يكون الوقت قد حان لبعض الإفصاح.

في شهر أكتوبر، الشهر ذاته الذي جرى فيه توقيع التوجيه الرئاسي بشأن العمليات السيبرانية «بي بي دي - 20»، رفعت وكالة الأمن القومي حظر النشر عن أحد أعداد مجلة «كريبتولوج» Cryptolog الذي مضى على صدوره خمسة عشر عاما، وهي مجلة تتناول تاريخ وسائل حرب المعلومات تصدرها الوكالة وتوزع داخليا. كان هذا العدد الخاص قد نشر في الربيع من العام 1997، وكانت محتوياته ممهورة بخاتم «سري جدا ويظلل» TOP SECRET UMBRA، دلالة على أنها من أكثر المواد حساسية التي تتناول استخبارات الاتصالات. أحد المقالات، كتبه «وليام بلاك»، أكبر مسؤولي وسائل حرب المعلومات في الوكالة في ذلك الوقت، أشار إلى أن وزير الدفاع كان قد فوض إلى وكالة الأمن القومي «سلطة تطوير[38] تقنيات مهاجمة شبكة الحاسوب (سي إن أيه)». في تذييل، استشهد بلاك بتوجيه وزارة الدفاع من العام الذي سبق، كان يعرف هجوم شبكات الحاسوب (سي إن أيه) على أنه «عمليات لعرقلة، أو حجب، أو إضعاف، أو تدمير المعلومات المستقرة في أجهزة الحواسيب وشبكاتها، أو أجهزة الحاسوب والشبكات ذاتها».

كان هذا - على نحو ملحوظ - مشابها للطريقة التي كان التوجيه الرئاسي المتعلق بالسياسات «بي بي دي - 20» الذي أصدره أوباما قد عرف بها (الأثر السيبراني) - على أنه «التلاعب، أو عرقلة، أو حجب، أو إضعاف، أو تدمير أجهزة الحاسوب، أو أنظمة المعلومات أو الاتصالات، أو الشبكات، أو البنية الأساسية المادية أو الافتراضية التي يجري التحكم فيها بواسطة الحواسيب أو نظم المعلومات، أو المعلومات المستقرة فيها».

بهذا المنطق، فإن التوجيه الرئاسي المتعلق بالسياسات «بي بي دي - 20» كان يعبِّر، بصياغة لغوية أكثر إسهابا نسبيا، عن الفكرة التي كانت موجودة منذ وسائل وليام بيري للحرب المضادة للقيادة والسيطرة في أواخر السبعينيات من القرن العشرين.

بعد كل تلك العقود، كان مقال مجلة كريبتولوج الذي رفعت عنه السرية، وصُرِّح بنشره، هو الذي وسم المرة الأولى التي كان قد ظهر في وثيقة عامة علانية مصطلح هجوم شبكات الحاسوب (سي إن أيه)، أو مثل هذا التعريف الدقيق للمفهوم.

في داخل سلاح الجو الذي كان دائما هو الفرع العسكري الأكثر نشاطا في الفضاء السيبراني، شرع كبار الضباط في كتابة بيان سياسة عامة يقر بقدراته في مهاجمة شبكات الحاسوب (سي إن أيه)، بقصد إصدار البيان للعامة، لكن بعد ذلك، بمجرد أن كانوا على وشك الانتهاء من المسودة، قضي الأمر. كان «ليون بانيتا» Leon Panetta، وهو عضو ديموقراطي سابق في الكونغرس، ومدير الموازنة الذي كان قد حل محل روبرت غيتس المرهق كوزير للدفاع في عهد أوباما، قد أصدر مذكرة تحظر أي إشارات لاحقة إلى البرامج الأمريكية التي تخص مهاجمة شبكة الحاسب (سي إن أيه).

كان أوباما قد قرر مواجهة الصينيين، على نحو مباشر، بشأن تغلغلهم المستشري في شبكات الحاسوب بالولايات المتحدة. ولم يكن بانيتا يرغب في أن يقدم ضباطه الدليل الذي ربما يساعد الصينيين على اتهام الرئيس الأمريكي بالرياء والنفاق.

13

عمليـة أدوات الوصول من بُعد الغامضة (عملية شِـدي رات)

«كان الروس يحاولون الحفاظ على سرية نشاطهم السيبراني، أما الصينيون فهم يفعلون ذلك ببساطة في كل مكان، علنا على الملأ، كأنهم لم يهتموا بما إذا كان أي أحد يلاحظ»

في يوم 11 مارس 2013 ألقى توماس دونيلون، مستشار الرئيس باراك أوباما للأمن القومي، كلمة في منظمة «مجتمع آسيا»، في الجانب الشرقي العلوي من مانهاتن. جزء كبير من كلمته كان نمطيا؛ سرد لسياسة الإدارة نحو «إعادة توازن وضعها العالمي»[1] بعيدا عن المعارك القديمة في الشرق الأوسط، وفي اتجاه المنطقة «الديناميكية النشطة» في آسيا والباسيفيك (المحيط الهادئ)، باعتبارها دفعة من أجل النمو والازدهار.

لكن بعد انقضاء نحو ثلثي الخطاب اخترق دونيلون آفاقا دبلوماسية جديدة. بعد أن سرد وعدّد بضعة «تحديات» تواجه العلاقات

الأمريكية - الصينية، قال: «ثمة قضية أخرى من هذا القبيل هي الأمن السيبراني»، مضيفا أن التعدي الصيني في هذا المضمار «أصبح يحتل صدارة جدول الأعمال».

استطرد دونيلون «كانت الشركات الأمريكية يساورها قلق متزايد إزاء السرقة المتطورة، والمحددة الأهداف، لمعلومات سرية تخص الأعمال، ولتكنولوجيات مشمولة بحقوق الملكية، من خلال عمليات تسلل سيبراني منطلقة من الصين على نطاق غير مسبوق».

ثم صعّد دونيلون الأمور أكثر ووضعها على المحك، قال: «بدءا من الرئيس إلى مَن دونه، لقد صارت هذه نقطة اهتمام رئيسي ومحورا للحوار مع الصين على كل مستويات حكومتينا، وستستمر كذلك. إن الولايات المتحدة ستبذل كل ما في وسعها لحماية شبكاتنا القومية، والبنية الأساسية الحرجة، وممتلكاتنا العامة والخاصة الثمينة».

قال دونيلون إن إدارة أوباما ترغب في أن تفعل بكين شيئين؛ أولا، أن تدرك وتقرّ «بالضرورة الملحّة لهذه المشكلة واتساعها والخطر الذي تشكله على التجارة الدولية، وعلى سمعة الصناعة الصينية، وعلى علاقاتنا بوجه عام»؛ ثانيا، «اتخاذ خطوات جادة نحو التحقيق في هذه الأنشطة ووضع حد لها».

كان المطلب الأول هو تهديدا هامشيا نوعا ما، غيِّر أساليبك أو جازف بتصدع علاقاتنا. كان الثاني محاولة لإعطاء القادة الصينيين مخرجا يحفظ ماء الوجه، فرصة للإلقاء بلائمة الاختراق على مثيري الشغب و«اتخاذ خطوات جادة» لوقفه.

الواقع أن دونيلون - وكل مسؤول آخر لديه تصريح أمني رفيع المستوى(*) - كان يعلم أن الجاني في هذه التسللات لم يكن عصابة من قراصنة الحاسوب (الهاكرز) المستقلين الذين يعملون لحسابهم الخاص، لكن بالأحرى كانت الحكومة الصينية ذاتها هي الجاني؛ تحديدا، المكتب الثاني من القسم الثالث لهيئة الأركان العامة لجيش التحرير الشعبي، المعروف أيضا باسم الوحدة 61398 في جيش التحرير الشعبي، التي كان مقرها في مبنى إداري أبيض يتكون من 12 طابقا في ضواحي شنغهاي Shanghai.

(*) تصريح أمني رفيع المستوى: هو ترخيص يُمنح للأشخاص للسماح لهم بالاطلاع على المعلومات المصنفة على أنها سرية وارتياد أماكن محظورة. [المترجم].

كان أوباما قد أثار القضية مرارا وتكرارا منذ بداية فترة رئاسته لكن على نحو هادئ، من أجل حماية المصادر والأساليب الاستخباراتية من ناحية، ومن ناحية أخرى لأنه كان يرغب في تحسين العلاقات مع الصين، وكان يرى أن المواجهة بشأن السرقة السيبرانية ستؤدي إلى عرقلة تلك الجهود. كان الديبلوماسيون الأمريكيون يطرحون الأمر باعتباره قضية جانبية في كل جلسة من جلسات «الحوار الاستراتيجي والاقتصادي» الآسيوي - الأمريكي الذي يعقد سنويا، وذلك بدءا من جلسات أوباما الأولى في العام 2009. لم تكن الوفود الصينية ترد بحدة أو تمسك عن الكلام في أي من هذه المناسبات، إلى حد أنهم كانوا دائما يتفقون في الرأي ويجيبون بأنه ينبغي للمجتمع الدولي أن يضع حدا لهذا السطو. وإذا أثار أحد الديبلوماسيين الأمريكيين تورط الصين ذاتها في الاختراق السيبراني كان الصينيون يدفعون الاتهام عنهم.

بعد ذلك في 18 فبراير نشرت شركة «مانديانت» Mandiant[2]، وهي شركة رائدة في مجال أمن الحاسوب، ومقرها مدينة «أَلِكسَندريا» Alexandria بولاية فرجينيا Virginia، تقريرا يتألف من ستين صفحة يحدد الوحدة 61398 بجيش التحرير الشعبي على أنها أحد أكثر القراصنة السيبرانيين إدهاشا في العالم. ذكر التقرير أنه على مدار الأعوام السبعة السابقة كان قراصنة الحاسوب في شنغهاي هم المسؤولين عما لا يقل عن 141 هجوما سيبرانيا ناجحا في عشرين قطاعا صناعيا رئيسيا، يتضمن مقاولي (متعهدي) الدفاع، والمنشآت المائية (محطات المياه)، وأنابيب النفط والغاز، والبنى الأساسية الحرجة الأخرى. كان هؤلاء القراصنة المخترقون يتسكعون داخل إحدى الشبكات المستهدفة طوال عام كامل، وفي إحدى الحالات طوال أربعة أعوام وعشرة أشهر، قبل أن يُكتشَفوا. أثناء عملية واحدة كانت على نحو خاص من دون عراقيل نهبوا 6.5 تيرا بايت من البيانات من شركة واحدة خلال عشرة أشهر.

كان كيفن مانديا Kevin Mandia - مؤسس شركة «مانديانت» ومديرها التنفيذي - هو أحد محققي سلاح الجو في جرائم الفضاء السيبراني، الذين نالوا من موسكو قبل خمسة عشر عاما وكشفوا أنها الجاني في عملية «متاهة ضوء القمر»، أول اختراق أجنبي جاد لحواسيب وزارة الدفاع. في الفترة نفسها تقريبا كان ريتشارد بيجليك Richard Bejtlich - كبير مسؤولي الأمن في «مانديانت» - هو اختصاصي دفاع شبكات الحواسيب في مركز سلاح الجو لوسائل حرب المعلومات، المركز الذي

ركّب أول أجهزة لرصد أمن الشبكات لكشف وتتبع عمليات النفاذ إلى الحواسيب العسكرية. كان نظام الرصد الذي بناه مانديا وبيجليك في «مانديانت» قائما على النظام الذي استخدمه سلاح الجو في سان أنطونيو.

بينما كان مانديا يلملم تقريره بشأن الوحدة 61398 تعاقدت معه «نيويورك تايمز» The New York Times للتقصي في اختراق قسم الأخبار لديها. بينما كان هذا التقصي يحرز تقدما (تبين أن المخترق كان منظمة حكومية صينية مختلفة) كان هو وناشرو الصحيفة يبحثون إمكانية اتفاق عمل طويل الأجل، لذا أعطاهم مانديا مسبقا نسخة أولية من التقرير بشأن وحدة شنغهاي. نشرت صحيفة «تايمز» Times مقالا طويلا على صفحتها الأولى[3] توجز فيه محتويات التقرير.

استنكرت وزارة الشؤون الخارجية الصينية الادعاءات باعتبارها ادعاءات «غير مسؤولة» و«غير مهنية» و«غير ذات فائدة لحل المشكلة المعنية»، وأضافت بذات الإنكار السريع الحاد الذي كان مسؤولوها يرددونه دائما في اجتماعاتهم مع الديبلوماسيين الأمريكيين، «الصين تعارض بشدة أعمال القرصنة الحاسوبية».

مع ذلك كان الصينيون في الواقع يمارسون القرصنة الحاسوبية بفجور متزايد على مدار أكثر من عقد. ذات مرة كان مسؤول رفيع المستوى في استخبارات الولايات المتحدة قد تمتم في إحدى جلسات مجلس الأمن القومي بأنه على الأقل كان الروس يحاولون الحفاظ على سرية نشاطهم السيبراني، أما الصينيون فهم يفعلون ذلك ببساطة في كل مكان، علنا على الملأ، كأنهم لم يهتموا بما إذا كان أي أحد يلاحظ.

في فترة مبكرة تعود إلى العام 2001[4]، في عملية أطلقت عليها دوائر الاستخبارات الأمريكية اسم «المطر الجبار» (Titan Rain)، اخترق المقاتلون السيبرانيون الصينيون شبكات العديد من القيادات العسكرية الغربية، والدوائر الحكومية، ومؤسسات الدفاع، ومختبرات الأبحاث، مستخدمين تقنيات تعيد إلى الأذهان عملية «متاهة ضوء القمر» التي نفذها الروس.

في الفترة ذاتها تقريبا تبنى القسم الثالث لهيئة الأركان العامة لجيش التحرير الشعبي الصيني - الذي أنشأ الوحدة 61398 فيما بعد – فقها جديدا أطلق عليه اسم «صِدام المعلومات»[5] (information confrontation)؛ وأُنشئت أقسام «أبحاث أمن المعلومات» في أكثر من خمسين جامعة صينية. وبحلول نهاية العقد[6]

بدأ الجيش الصيني في دمج الأدوات والتقنيات السيبرانية في تدريبات بأسماء، مثل: «القبضة الحديدية» (Iron Fist)، و«مهمة هجوم» (Mission Attack). في أحد السيناريوهات كان جيش التحرير الشعبي يخترق شبكات القيادة والسيطرة الخاصة بسلاح الجو الأمريكي وسلاح البحرية الأمريكية، في محاولة لعرقلة ردها على احتلال تايوان.

باختصار كان الصينيون يقلدون عقيدة «وسائل حرب المعلومات» الأمريكية، مما يبرهن، مجددا، الدرس الذي تعلمه الكثيرون ممن اكتشفوا أن فنون السيبرانية هي في البداية مغرية، ثم تنذر بالخطر، ما كان يمكننا فعله بأحد الخصوم، فإن أحد خصوم كان يمكنه فعله بنا.

كان هناك اختلاف واحد كبير في الهجمات السيبرانية الصينية، إذ إنهم لم يكونوا يمارسونه للتجسس وتمهيد ساحة المعركة فقط، ولكن أيضا لسرقة الأسرار التجارية، والممتلكات الفكرية، والأموال.

في العام 2006، إن لم يكن قبل ذلك، بدأ كثير من مكاتب السيبرانية التابعة للجيش الصيني في اختراق مجموعة واسعة من الشركات في كل أرجاء العالم. بدأت الحملة بسلسلة من الغارات على مقاولي (متعهدي) الدفاع، كان أبرزها قرصنة ضخمة لشركة «لوكهيد مارتن» Lockheed Martin، حيث سرقت الصين عشرات الملايين من وثائق تخص طائرة الضربات الاستباقية المقاتلة «إف-35» التي تصممها الشركة. لم يكن أي من الملفات مصنفا على أنه سريّ، لكنها كانت تحتوي على بيانات ومخططات لتصميمات أولية بشأن تصميم مقصورة القيادة، وإجراءات الصيانة، وتكنولوجيا التخفي، وأمور أخرى كان بإمكانها مساعدة الصينيين على التصدي للطائرة في المعركة، أو في الوقت ذاته، بناء الصين نسختها المقلدة من الطائرة «إف-35» (وهذا ما فعلوه في نهاية المطاف).

على نحو خاص انزعج الكولونيل غريغوري راتراي Gregory Rattray، قائد مجموعة في مركز سلاح الجو لوسائل حرب المعلومات (الذي كان اسمه قد تغير أخيرا إلى مركز سلاح الجو لعمليات المعلومات)، ليس فقط بسبب جسامة وضخامة غارات الصين السيبرانية، ولكن أيضا بسبب الموقف السلبي للمؤسسات الأمريكية. كان راتراي من ذوي الخبرة والمهارة الفائقة في هذا الميدان، إذ إنه كان قد كتب أطروحة عن وسائل حرب المعلومات لنيل درجة الدكتوراه[7] من «كلية فليتشر

للقانون والدبلوماسية»، وعمل ضمن فريق ريتشارد كلارك في الأعوام الأولى من فترة رئاسة جورج دبليو بوش، ثم بعد استقالة كلارك بقي في البيت الأبيض في منصب مدير الأمن السيبراني.

في أبريل 2007 استدعى راتراي عدة مديرين تنفيذيين من أكبر مقاولي (متعهدي) الدفاع بالولايات المتحدة، وأخبرهم بأنهم يعيشون في عالم جديد. كانت تقديرات الاستخبارات التي ألصقت الهجمات السيبرانية بالصين سرية جدا. لذلك نحت راتراي في إحدى لوحات عرض إحاطته مصطلحا لوصف تصرفات وأفعال قرصان الحاسوب (الهاكر) على أنها «آيه بي تي» APT وتعني: «تهديدا متقدما دائما» (Advanced Persistent Threat). كانت دلالتها حرفيا هي أن قرصان الحاسوب يستخدم تقنيات متطورة، وكان يبحث عن معلومات محددة، وكان يبقى داخل النظام – أسابيع، وحتى أشهر - مادام ذلك ضروريا للعثور عليها. (اعتُمِد المصطلح وانتشر؛ وبعد مضي ستة أعوام، وضع كيفن مانديا عنوانا لتقريره، هو: «آيه بي تي 1» APT1.

كانت القرصنة الصينية النمطية تبدأ[8] برسالة للتصيد الاحتيالي الموجه (spear-phishing email) ترسل بالبريد الإلكتروني إلى موظفي الشركة المستهدفة. إذا نقر موظف واحد فقط على المرفق المرتبط برسالة البريد الإلكتروني (وكل ما يتطلب الأمر هو موظف واحد)، كان الحاسوب ينزل صفحة ويب مكتظة ببرامج خبيثة، بما في ذلك الفيروس الحاسوبي «حصان طروادة للوصول من بُعد» (Remote Access Trojan)، المعروف تجاريا بأنه «رات» (RAT). كان «رات» يفتح أحد الأبواب، مما يسمح للمتسللين بالتجوال في الشبكة، والحصول على امتيازات مسؤول النظم (systems administrator)، واستخلاص البيانات التي يريدونها. فعل المخترقون ذلك مع مؤسسات اقتصادية من مختلف الأنواع، بنوك (مصارف)، وخطوط أنابيب النفط والغاز، والمحطات المائية، ومديري بيانات الرعاية الصحية؛ أحيانا لسرقة أسرار، وأحيانا لسرقة أموال، وأحيانا لدوافع لم يكن من الممكن التحقق منها.

كانت شركة «ماكافي» McAfee لمكافحة فيروسات الحاسوب هي التي اكتشفت وتتبعت عملية القرصنة الصينية، وأطلقت على هذه العملية اسم «عملية شادي رات» (عملية أدوات الوصول من بُعد الغامضة Operation Shady RAT). على مدى الأعوام الخمسة المنتهية في العام 2011، حينما أطلعت شركة «ماكافي» البيت

الأبيض والكونغرس على النتائج التي توصلت إليها، سرقت «عملية شادي رات» بيانات ما يزيد على سبعين كيانا – دوائر حكومية وشركات خاصة - في أربع عشرة دولة، متضمنة الولايات المتحدة، وكندا، وعدة دول في أوروبا، والمزيد في آسيا، والعديد من الأهداف في تايوان؛ لكن، لا شيء في جمهورية الصين الشعبية، مما كان له مغزاه.

لم يكن الرئيس أوباما في حاجة إلى أن تخبره شركة «ماكافي» بشأن الفورة السيبرانية للصين، كانت دوائر الاستخبارات لديه تقدم له تقارير مماثلة. لكن حقيقة أن شركة تجارية لمكافحة فيروسات الحاسوب كانت قد تتبعت الكثير من أعمال القرصنة الحاسوبية، وأصدرت مثل هذا التقرير المفصل، جعلت من الصعب إبقاء القضية حبيسة داخل الغرفة الصغيرة المعزولة الخاصة بمؤتمرات القمة الدبلوماسية. أيضا كانت الشركات التي اختُرقت ستفضل أن تلتزم الصمت، إذ لا جدوى من إزعاج العملاء وحملة الأسهم. لكن سرعان ما انتشر الخبر، وكان رد فعل الشركات هو الضغط على البيت الأبيض لفعل شيء؛ لأسباب كان أهمها هو أنه، بعد كل هذه العقود من التحليلات والتحذيرات، فالعديد منهم لايزال يجهل ما الذي يمكنه فعله بذاته.

كانت هذه هي الظروف المحيطة التي غلت يدي أوباما. بعد قمة أمنية آسيوية أخرى، حيث أثار الدبلوماسيون الأمريكيون القضية مجددا، ومجددا نفى الصينيون تورطهم، طلب أوباما من توم دونيلون أن يلقي خطابا ليخرج القضية إلى الملأ. وكان مما أسهم في زيادة الضغط وتعجيل الجدول الزمني، تقرير شركة «مانديانت» الذي قد نشر قبل ذلك بثلاثة أسابيع، لكن كانت العجلة قد دارت.

كانت إحدى فقرات خطاب دونيلون قد سببت إزعاجا لبعض المسؤولين الرسميين في المستوى المتوسط، لاسيما في البنتاغون. واصفا الغارات الهجومية السيبرانية على أنها انتهاك للمبادئ العمومية الشائعة، باعتبارها أمرا أشبه بسبب لاندلاع الحرب، أعلن دونيلون: «المجتمع الدولي لا يسعه تحمل التسامح مع أي نشاط من هذا القبيل من أي دولة».

تحير مسؤولو البنتاغون وفكروا في الأمر مليا، «أي نشاط من هذا القبيل من أي دولة»؟ كانت الحقيقة، وكان الجميع يعرفها، هي أن الولايات المتحدة أيضا متورطة

في هذا النشاط. كانت أهدافها مختلفة، إذ لم تكن دوائر الاستخبارات الأمريكية تسرق أسرارا تجارية، أو مخططات لتصميمات أولية تخص شركات أجنبية، فضلا عن أموالها النقدية. ويرجع ذلك أساسا إلى أنهم لم يكونوا في حاجة إلى ذلك. لم تكن مثل هذه الأسرار أو المخططات ستضيف إلى الشركات الأمريكية أفضلية، هم كانت لديهم الأفضلية بالفعل.

في اجتماعات مجلس الأمن القومي بشأن الموضوع كان معاونو البيت الأبيض يدفعون ويجادلون بأن هذه التفرقة كانت مهمة، إذ إن التجسس من أجل الأمن القومي كان ممارسة قديمة ومقبولة. لكن إذا كان الصينيون يرغبون في الانضمام إلى الاقتصاد الدولي، كان لزاما عليهم احترام حقوق الملكية، بما في ذلك الملكية الفكرية. لكن مسؤولين آخرين في تلك الاجتماعات كانوا يتساءلون عما إذا كان هناك اختلاف فعلي. كانت وكالة الأمن القومي تخترق الشبكات الصينية للمساعدة على إلحاق الهزيمة بهم في الحرب، وكانت الصين تخترق الشبكات الأمريكية أساسا للمساعدة على إثراء اقتصادها. ما الذي جعل أحد أشكال القرصنة مسموحا به والشكل الآخر غير مقبول ولا يمكن تحمله؟

حتى إن كان لدى مساعدي البيت الأبيض وجهة نظر (وكان مسؤولو البنتاغون يسلمون بأنهم كانوا كذلك)، ألم تكن الإدارة على حافة الخطر بالإعلان عن هذا الانتقاد؟ ألن يكون من السهل جدا على الصينيين الإفراج عن سجلاتهم الخاصة ونشرها كاشفين أننا أيضا كنا نخترقهم، ومن ثم يتهموننا بالرياء والنفاق؟ إن جزءا مما كنا نفعله كان دفاعيا، إذ إن النفاذ إلى شبكاتهم كان من أجل متابعتهم وهم ينفذون إلى شبكاتنا؛ ونحن كنا ننفذ إلى عمق هذه الشبكات لدرجة أنه حينما كان الصينيون يحاولون اختراق أنظمة وزارة الدفاع (أو، في الآونة الأخيرة، أنظمة العديد من مقاولي الأسلحة أيضا)، كانت وكالة الأمن القومي ترصد كل خطوة يتخذونها، كانت ترصد ما كان الصينيون يرونه على شاشاتهم الخاصة. في بضع مناسبات ما كان الصينيون يسرقونه من أسرار تصنيع، لم يكن في حقيقته أسرارا على الإطلاق، كانت مخططات لتصميمات أولية وهمية زائفة غرستها وكالة الأمن القومي في مواقع معينة على أنها آنية عسل. لكن تلك العمليات السيبرانية كانت إلى حد ما ذات طبيعة هجومية، إذ إن الولايات المتحدة كانت تنفذ إلى الشبكات الصينية من أجل الإعداد للمعركة،

لاستغلال مواطن الضعف وممارسة السيطرة، تماما مثلما كان يفعل الصينيون، وتماما مثلما كانت تفعل دائما كل القوى العظمى في مختلف مجالات وسائل الحرب.

كان من الواضح أن انتقاد الصين بسبب القرصنة هو برمته أمر أخرق وغير ملائم، نظرا إلى ما تكشف أخيرا بشأن عملية «ستوكسنت»، فضلا عن توقيع أوباما أخيرا للتوجيه الرئاسي بشأن العمليات السيبرانية «بي بي دي20-» (على الرغم من أنه لايزال سريا). أقر بعض معاوني أوباما في البيت الأبيض بوجود بعض التعارض في الموقف، كان ذلك هو أحد الأسباب التي جعلت الإدارة ترفض الاعتراف بأنها كانت تؤدي دورا في عملية «ستوكسنت»، بعد فترة طويلة من انكشاف أمر العملية.

في شهر مايو طار دونيلون إلى بكين لوضع ترتيبات لعقد قمة بين الرئيس أوباما ونظيره الصيني شي جين بينج Xi Jinping. أوضح دونيلون أن موضوع السيبرانية سيكون على جدول الأعمال، وإذا لزم الأمر، فإن أوباما كان سيُطلع «شي» على حجم ما عرفته استخبارات الولايات المتحدة بشأن الممارسات الصينية. كان من المقرر عقد القمة في مدينة رانشو ميراج Rancho Mirage بولاية كاليفورنيا، في حوزة قطب الإعلام الراحل والتر أنيبنبرغ Walter Annenberg، في يومي الجمعة والسبت، 7 و8 يونيو 2013.

في يوم 6 يونيو نشرت صحيفتا «واشنطن بوست» The Washington Post و«الغارديان» The Guardian اللندنية[9]، في تقارير كبيرة على الصفحة الأولى، أن وكالة الأمن القومي و«مقر الاتصالات الحكومية البريطانية» (جي سي إتش كيو) كانا ينقِّبان منذ زمن طويل في بيانات تسع من شركات الإنترنت ضمن برنامج سري جدا يعرف باسم «بريزم» (PRISM). وغالبا ما كان ذلك يحدث بموجب قرارات سرية من المحكمة، وأنه من خلال هذا البرنامج وغيره، كانت وكالة الأمن القومي تجمع سجلات الهاتف لملايين المواطنين الأمريكيين. تلك كانت هي التقارير الأولى[10] من العديد من التقارير الصحافية، التي نشرت على مدار الأشهر الكثيرة التالية في صحف «الغارديان»، و«بوست» Post، و«دير شبيغل» Der Spiegel، وغيرها في نهاية المطاف؛ مستندة إلى خبيئة ضخمة من الوثائق فائقة السرية كان مسؤول النظم في وكالة الأمن القومي، إدوارد سنودن Edward Snowden، قد اختلسها من حاسوبه في مبنى الوكالة في جزيرة أواهو Oahu

بولاية هاواي Hawaii، وسرّبها إلى ثلاثة صحافيين قبل أن يفر إلى هونغ كونغ Hong Kong، حيث التقى مع اثنين منهم، هما لورا بويتراس Laura Poitras وغلين غرينوالد Glenn Greenwald (المراسل الآخر، بارتون جيلمان Barton Gellman، لم يتمكن من اللحاق بهم هناك).

جاء التسريب عشية قمة «أوباما - شي». وعلى الرغم من ذلك، كاد هذا التوقيت يكون مؤكدا أنه مصادفة؛ لأن سنودن كان على اتصال مع المراسلين طوال شهور. لكن التسريب كان له تأثير كارثي مدمر. أحضر أوباما موضوع السرقة السيبرانية الصينية، وأخذ «شي» نسخة من صحيفة الغارديان. من تلك النقطة فصاعدا، فإن الرد الصيني السريع القاطع[11] على كل الاتهامات الأمريكية بشأن هذا الموضوع تحول من «نحن لا نضطلع بالقرصنة» إلى «أنتم تفعلون ذلك أكثر مما نفعله نحن».

بعد أسبوع واحد من القمة الفاشلة[12]، وكأنه تعزيز لموقف «شي»، قال سنودن في مقابلة مع صحيفة «ساوث تشاينا مورنينغ بوست» South China Morning Post، أكبر صحيفة في هونغ كونغ، إن وكالة الأمن القومي أطلقت أكثر من 61 ألف عملية سيبرانية، متضمنة اعتداءات على مئات الحواسيب في هونغ كونغ والقارة الصينية. قبل هذا الوقت، وفي مقطع فيديو مثير سجله الصحافي بويتراس في غرفته بالفندق، كان سنودن قد كشف عن أنه هو مصدر التسريبات.

كانت مقابلة صحيفة «مورننغ بوست» سببا في إثارة الشكوك بشأن دوافع سنودن، فهو لم يعد يفضح أمر تجاوزات ومفاسد ما تضطلع به وكالة الأمن القومي من مراقبة محلية فقط، بل كان أيضا يفضح أمر عمليات الاستخبارات الأجنبية. سرعان ما جاءت القصص والتقارير الصحافية[13] بشأن اختراق وكالة الأمن القومي لحركة البريد الإلكتروني واتصالات الهاتف الجوال لمتمردي حركة طالبان على الحدود الشرقية لأفغانستان، وهي كانت عملية لقياس ولاءات مجندي وكالة الاستخبارات المركزية في باكستان؛ واعتراضات البريد الإلكتروني لمساعدة التقديرات الاستخباراتية للأحداث في إيران؛ وبرنامج مراقبة لاتصالات الهواتف الجوالة «في جميع أنحاء العالم»، بهدف العثور على شركاء للإرهابيين المعروفين وتتبعهم.

كان أحد التسريبات يتألف من خمسين صفحة هي القائمة الكاملة للأدوات والتقنيات التي كان يستخدمها صفوة المخترقين في «مكتب عمليات الولوج المصممة

وفقا للحاجة» (تاو - تي إيه أوو) التابع لوكالة الأمن القومي. لم تنشر أي صحيفة أمريكية أو بريطانية تلك الوثيقة، على الرغم من أن صحيفة «دير شبيغيل» نشرتها في إصداراتها المطبوعة والإلكترونية. الآن تبعثرت جواهر التاج التي تخص «فورت ميد»[14] في كل أرجاء الشارع العالمي، متاحة ليلتقطها أي من الأطراف المهتمة أينما كانوا. حتى المواد التي لم ينشرها أحد – وكانت خبيئة سنودن تصل إلى عشرات الآلاف من الوثائق السرية جدا - كان من الممكن أن يكون قد أطلع عليها أي جهاز استخبارات أجنبي لديه وحدات سيبرانية ماهرة متمرسة. إذا كانت وكالة الأمن القومي ومثيلاتها الروسية، والصينية، والإيرانية، والفرنسية، والإسرائيلية، تستطيع كل منها اختراق حواسيب الأخريات، فمن المؤكد أنها كانت تستطيع اختراق حواسيب الصحافيين، الذين كان بعضهم أقل حذرا من الآخرين في حراسة الخبيئة. حالما أخذ سنودن حاسوبه المحمول خارج البناية في «أواهو»، فإن محتوياته - مشفرة أو غير مشفرة - أصبحت عرضة للاستيلاء عليها.

لكن التسريبات بشأن العمليات الاستخباراتية الخارجية - اعتراضات البريد الإلكتروني في أفغانستان وباكستان، وقائمة أدوات وتقنيات «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو)، وما شابه ذلك - حُجبت فيما بين قراء الصحف الأمريكيين، بواسطة الحسابات التفصيلية للمراقبة المحلية. كانت تلك التسريبات هي السبب في الإطراء على سنودن باعتباره شخصا يلفت نظر الآخرين إلى التجاوزات والمفاسد بقصد وضع حد لها، وغمرت وكالة الأمن القومي بعاصفة من الجدل والاحتجاج لم تشهدها منذ جلسات استماع لجنة «تشيرش»[*] في سبعينيات القرن العشرين.

أسقطت أوراق سنودن النقاب عن عملية هائلة للتنقيب في البيانات، أكثر اتساعا مما كان أي شخص خارجي قد تخيله. إنها عمليا كانت تجربة البيانات

(*) لجنة تشيرش Church Committee هي لجنة مختارة من مجلس الشيوخ بالولايات المتحدة الأمريكية لدراسة العمليات الحكومية فيما يتعلق بأنشطة الاستخبارات، وهي لجنة برئاسة سيناتور ولاية أيداهو Idaho «فرانك تشيرش» Frank Church في العام 1975. وقد حققت اللجنة في الانتهاكات التي ارتكبتها وكالة الاستخبارات المركزية، ووكالة الأمن القومي، ومكتب التحقيقات الفدرالي، وخدمة الإيرادات الداخلية. وكانت اللجنة جزءا من سلسلة من التحقيقات في انتهاكات الاستخبارات في العام 1975 الذي أطلق عليه «عام الاستخبارات». أدت جهود اللجنة إلى إنشاء لجنة دائمة مختصة بمجلس الشيوخ الأمريكي للاستخبارات. [المترجم].

الواصفة التي اضطلع بها كيث ألكسندر في «فورت بيلفواير» Fort Belvoir في أوضح وأشمل صورها، والتطبيق لفلسفته بشأن البيانات الضخمة، وهي اجمع وخزن كل شيء، بحيث يمكنك العودة والبحث عن أنماط وقرائن لهجوم وشيك. إنك حينما تبحث عن إبرة في كومة قش، فأنت بحاجة إلى كومة القش بكاملها.

في إطار نظام المراقبة الذي وصفته[15] وثائق سنودن، كانت وكالة الأمن القومي حينما تكتشف أن أحد الأشخاص على اتصال بإرهابيين أجانب، كان محللوها يمكنهم العودة إلى الوراء والنظر في كل رقم هاتف كان الشخص المشتبه فيه قد اتصل به (وكل رقم كان قد اتصل بالمشتبه فيه) طوال الأعوام الخمسة السابقة. كان استرجاع جميع تلك الأرقام ذات الصلة يسمى «القفزة» الأولى. لتوسيع التقصي بعد ذلك، كان في إمكان المحللين النظر في كل الأرقام التي كان هؤلاء الأشخاص قد اتصلوا بها (القفزة الثانية)؛ وفي قفزة ثالثة، الأرقام التي كان هؤلاء الأشخاص قد اتصلوا بها.

تشير الرياضيات، ولو فرضيا على الأقل، إلى مستوى صاعق من المراقبة. تخيل أن شخصا ما كان قد اتصل هاتفيا برقم عضو معروف في تنظيم القاعدة، وافترض أن هذا الشخص كان قد اتصل هاتفيا بمائة شخص آخر على مدار الأعوام الخمسة الماضية. كان ذلك سيعني أن وكالة الأمن القومي كان يمكنها أن تبدأ في تعقب ليس فقط الاتصالات الهاتفية للمشتبه فيه، ولكن أيضا الاتصالات الهاتفية لهؤلاء الأشخاص المائة الآخرين. إذا اتصل كل فرد من هؤلاء الأشخاص أيضا بمائة شخص، فإن وكالة الأمن القومي كان يمكنها - في القفزة الثانية - تعقب مكالماتهم أيضا، وذلك كان سيضع (100 ضرب 100) 10 آلاف شخص تحت فحص الوكالة. في القفزة الثالثة، كان في إمكان المحللين تتبع مكالمات الأشخاص العشرة آلاف والاتصالات الهاتفية التي أجروها - أو (10 آلاف ضرب 100) أي مليون شخص.

بعبارة أخرى، المراقبة النشطة الإيجابية لشخص واحد مشتبه في أنه إرهابي، كان يمكن أن تؤدي إلى وضع مليون شخص، على الأرجح مليون أمريكي، تحت مراقبة الوكالة. جاء هذا الانكشاف بمنزلة صدمة، حتى بالنسبة إلى أولئك الذين لم يكن لديهم سوى بضعة هواجس بشأن خرق الخصوصية الشخصية العرضي العابر.

بعد هذا الإفشاء[16]، ألقى كيث ألكسندر الكثير من الخطب، وأجرى عدة مقابلات صحافية، أكد فيها أن وكالة الأمن القومي لم تكن تفحص محتويات تلك

الاتصالات، أو أسماء المتصلين (كانت تلك المعلومات تُستبعد من قاعدة البيانات على نحو منتظم)، لكن بدلا من ذلك كانت تفحص البيانات الواصفة فقط، مثل: أنماط حركة البيانات - أي من أرقام الهواتف اتصل بأي من أرقام الهواتف الأخرى - إلى جانب تواريخ، وتوقيتات ومدة تلك الاتصالات.

لكن في خضم القصص والتقارير الإخبارية المثيرة، جاء تأكيد من مدير وكالة الأمن القومي ليضرب وترا حساسا، ربما ألكسندر يقول إن وكالته لم تستمع إلى هذه الاتصالات الهاتفية، لكن كان الكثير يتساءلون: لماذا كان عليهم تصديقه؟

تعمق انعدام الثقة حينما ضُبط مدير الاستخبارات القومية في عهد أوباما، جيمس كلابر James Clapper، متورطا في كذبة، وهو ليوتينانت جنرال (فريق) متقاعد في سلاح الجو، وخبير محنك في مختلف دوائر التجسس. في السابق في 12 مارس، أي قبل ثلاثة أشهر من سماع أي شخص بشأن البيانات الواصفة، أو برنامج «بريزم» PRISM، أو إدوارد سنودن، أدلى كلابر بشهادته في جلسة استماع علنية أمام لجنة مجلس الشيوخ المختارة المعنية بالاستخبارات. عند نقطة ما، سأله عضو مجلس الشيوخ السيناتور رون وايدن Ron Wyden، وهو ديموقراطي من ولاية أوريغون Oregon: «هل تجمع وكالة الأمن القومي على الإطلاق[17] أي نوع من البيانات عن ملايين أو مئات الملايين من الأمريكيين؟».

أجاب كلابر: «لا يا سيدي... ليس عن عمد».

كان وايدن، بصفته عضوا في اللجنة المختارة، قد اطلع على برنامج وكالة الأمن القومي للبيانات الواصفة؛ لذلك، كان يعرف أن كلابر لم يكن يقول الحقيقة. في اليوم السابق، كان وايدن قد أعطى مكتب كلابر[18] تنبيها بشأن السؤال الذي كان يخطط لطرحه. كان يعلم أنه كان سيضع كلابر في مأزق، إذ إن الإجابة الصحيحة عن سؤاله هي «نعم»، لكن كلابر كان سيواجه صعوبة في قول ذلك من دون أن يصير مادة للعناوين الرئيسية للصحف؛ لذا، أراد وايدن أن يعطي المدير فرصة لصياغة إجابة تتناول القضية من دون أن تكشف الكثير. اندهش وايدن من أن كلابر تعامل معها بأن يكذب ببساطة. بعد جلسة الاستماع اقترب أحد معاوني وايدن من كلابر لسؤاله عما إذا كان سيرغب في مراجعة وتمديد رده من أجل السجلات، وتفاجأ وايدن ثانية، لقد امتنع كلابر. لم يكن وايدن يستطيع أن يقول علنا أي شيء إضافي آخر من دون

خرق تعهده بالحفاظ على هدوئه والتزام الصمت بشأن الأسرار رفيعة المستوى؛ لذا أوقف استمرار المناقشة وترك المسألة على حالها.

ثم جاءت مكاشفات سنودن، التي دفعت الكثيرين إلى إعادة النظر في تلك المقايضة. في 9 يونيو، يوم الأحد الأول بعدما نُشرت تسريبات سنودن، وافق كلابر على إجراء مقابلة تلفزيونية مع أندريا ميتشل Andrea Mitchell من قناة تلفزيون «إن بي سي - تي في NBC-TV». سألته ميتشل لماذا أجاب عن سؤال وايدن بتلك الطريقة.

ظهر كلابر غير متهيئ على نحو مدهش، بدأ كلامه بثرثرة على نحو استطرادي غير متسق: «أنا ظننت، وإن كان هذا تأمُّلا في الماضي[19]، أنني سئلت سؤالا ملغوما من نوعية «متى سوف... تتوقف عن ضرب زوجتك»، وهو سؤال... لا تكون بالضرورة الإجابة عنه ببساطة نعم أو لا». بعد ذلك، انزلق بنفسه أكثر عمقا في هذا الموقف الصعب المحرج، فقال: «لذا، أجبت بما اعتقدت أنه الأكثر واقعية وصدقا - أو الأقل زيفا – بأن قلت، لا».

تأكيدا لانزلاقه، ركز كلابر على استخدام وايدن لكلمة «جمع»، كما في «هل كانت وكالة الأمن القومي تجمع أي نوع من البيانات... بشأن الملايين من الأمريكيين؟»، قال كلابر، تخيل أن مكتبة شاسعة فيها كتب تحتوي على كميات هائلة من البيانات بشأن كل أمريكي، واستطرد قائلا: «بالنسبة إليّ، جمع بيانات أشخاص تابعين للولايات المتحدة كان سيعني إخراج الكتاب من الرف وفتحه وقراءته». ومن ثم، برر كلابر أنها لم تكن كذبة تماما أن نقول إن وكالة الأمن القومي لم تجمّع بيانات بشأن الأمريكيين، على الأقل ليس عمدا.

في صباح اليوم التالي لإذاعة المقابلة، اتصل كلابر بصديقه القديم كين مينيهان، المدير السابق لوكالة الأمن القومي، ليسأله عن رأيه في المقابلة التلفزيونية التي أجراها. كان مينيهان قد أصبح حاليا المدير الإداري لـ «مجموعة بالادين كابيتال» Paladin Capital Group، التي كانت تستثمر في شركات تكنولوجيا الأمن السيبراني في جميع أنحاء العالم، وكان قد خرج من الحكومة منذ أكثر من عقد، لكنه حافظ على اتصالاته وعلاقاته في أرجاء عالم الاستخبارات. كان لايزال مشاركا في اللعبة بقوة، وكان قد شاهد مقابلة كلابر بأسف وأسى.

أجاب مينيهان بلكنته الشعبية: «حسنا، لم يكن في إمكانك أن تجعل الأمور أسوأ».

ربما كان كلابر بالفعل مرتبكا ومشوش الذهن. قبل ذلك بخمسة أعوام، كانت «محكمة قانون مراقبة الاستخبارات الأجنبية» قد سمحت لوكالة الأمن القومي بإعادة تعريف كلمة «تجمّع» تماما بالطريقة ذاتها التي كان كلابر قد قدمها على التلفزيون الوطني، على أنها استرجاع لبيانات التُقطت وجُمعت وخُزنت. في وقت ذلك القرار الصادر عن المحكمة، كان ألكسندر يرسي الأساس لبرنامجه الخاص بالبيانات الواصفة، وكان من غير القانوني «جمع» البيانات عن الأمريكيين، لذلك لم يكن في إمكان البرنامج المضي قدما من دون إعادة تعريف المصطلح.

لكن محكمة قانون مراقبة الاستخبارات الأجنبية كانت هيئة سرية، إذ إنها كانت تجتمع سرا، وتستمع لقضاياها سرا، وكانت أحكامها وأوامرها مصنّفة على أنها سرية جدا. بالنسبة إلى كلابر وغيره من قدامى الخبراء في الأوساط الاستخباراتية، فإن هذا التجديد وإعادة صياغة كلمة شائعة في اللغة الإنجليزية شق طريقه باعتباره مصطلحا رسميا للتعبير. أما بالنسبة إلى أي شخص خارج الأوساط الاستخباراتية، فبدا المنطق أن أقل ما يقال عنه إنه مخادع. على نحو واضح، كانت كلمة «جمع» تعني: لملمة، اجتراف، ضم. لم يكن أحد سيقول: «أنا سأجمع رواية جاتسبي العظيم The Great Gatsby من رف الكتب الخاص بي وقراءتها»، ولا يبدو من المعقول أن أي شخص في وكالة الأمن القومي كان سيقول: «سأجمع هذه المحادثة الهاتفية من الأرشيف الخاص بي وأُدرجها في قاعدة بياناتي».

كانت وكالة الأمن القومي منذ لحظة تأسيسها ولفترة طويلة، قد حظيت بتكتم تام، حتى إن المنتمين إليها كانوا ينزعون إلى فقدان التواصل مع العالم الخارجي. من ناحية، كانت عزلتها نتاجا للمهمة المنوطة بها، إذ إن العمل في إعداد وتجهيز وكسر (فك) الشفرات من أجل مصلحة الأمن القومي كان يُصنف في جميع الدوائر الحكومية على أنه ضمن المهمات الأكثر حساسية، والمصنفة على أنها سرية. مع ذلك، فإن عزلتهم وتقوقعهم على ذاتهم تركهم من دون دفاعات حينما تكشفت الحقائق على نحو مفاجئ. لم يكن لديهم أي تدريب أو خبرة في التعامل في العلن مع العامة. وبينما كانت الأسرار الموجودة في

وثائق سنودن متناثرة وتحتل العناوين الرئيسية للصفحات الأولى من الصحف ونشرات الأخبار غداة اليوم الذي سبب دهشة كبيرة إلى حد الذهول، بدأ انهيار الثقة بأكبر دائرة استخبارات في البلاد، وأكثرها تدخلا، وهي ثقة لم تكن قط أكثر من كونها ثقة هشة واهية.

لم تكن استطلاعات الرأي هي الموضع الوحيد الذي تعرضت فيه الوكالة للهزيمة. جاء التقريع أيضا – وكان أيضا أكثر إضرارا - في التصريحات المنفعلة الثائرة، والاتصالات الهاتفية الغاضبة من الشركات الأمريكية؛ لاسيما مزودي خدمات الاتصالات والإنترنت، الذين كانت وكالة الأمن القومي قد استغلت شبكاتهم ومخدماتهم لتمتطيها وتتسرب من خلالها طوال أعوام، وفي بعض الحالات طوال عقود.

كان هذا الاتفاق بالنسبة إلى عديد من الشركات ذا منفعة متبادلة. في وقت قريب يرجع إلى العام 2009، بعد أن شن الصينيون هجوما سيبرانيا كبيرا على شركة غوغل Google، وسرقوا التعليمات البرمجية المصدر (كود المصدر) لبرمجيات الشركة، جواهر التاج لأي شركة إنترنت، حينئذ ساعدت مديرية ضمان المعلومات بوكالة الأمن القومي على إصلاح الضرر. قبل ذلك بعام واحد، بعد أن رفض سلاح الجو الأمريكي نظام التشغيل «إكس بي» XP من شركة مايكروسوفت Microsoft بذريعة أنه يعج بأوجه القصور والثغرات الأمنية، كانت المديرية تساعد الشركة على تصميم الإصدار الثالث من حزمة الخدمة لنظام التشغيل «إكس بي» XP (XP Service Pack 3)، أحد أنجح أنظمة الشركة، والتي كان التقنيون في سلاح الجو (والكثير من المستهلكين) يعتبرونها آمنة مسبقا ولا تحتاج إلى شيء وجاهزة للاستخدام مباشرة.

لكن الآن، مع تعري تواطئهم في المؤامرة، وانكشافه بوضوح ليراه الجميع، تراجع المسؤولون التنفيذيون لهذه الشركات، كان بعضهم يولول محتجا، مثل «كابتن رينو» Captain Renault، وهو مسؤول فيشي Vichy official في فيلم «كازابلانكا» Casablanca الذي أعلن بنفسه: «صُدمت، صُدمت باكتشافي أنه يجري لعب القمار هنا»، فقط في الوقت الذي كان

مدير صالة القمار يسلمه أرباح هذه الليلة. كانت خشيتهم هي أن العملاء في السوق العالمية ربما سيتوقفون عن شراء برمجياتهم، ويشتبهون في أنها كانت ممتلئة بأبواب خلفية لكي تتسلل منها وكالة الأمن القومي. وكما قال هاورد تشارني Howard Charney، النائب الأول لرئيس شركة سيسكو، وهي شركة أنجزت أعمالا كثيرة مع وكالة الأمن القومي، قال لأحد الصحافيين، إن مكاشفات سنودن كانت «تلطيخا لسمعة[20] الشركات الأمريكية الأصل حول العالم».

كانت حكومات الدول الحليفة حول العالم تصرخ هي أيضا. الدول الناطقة بالإنجليزية التي كانت تتشارك المعلومات الاستخباراتية مع الولايات المتحدة على مدار عقود من الزمن - دول «العيون الخمس»، بريطانيا العظمى، وكندا، وأستراليا، ونيوزيلندا – بقيت ثابتة واتخذت موقفا حاسما. لكن زعماء الدول الأخرى، الذين لم يكن قد سمح لهم بالانضمام إلى الركب، بدأوا في الابتعاد والمراوغة. كان الرئيس أوباما قد خطط لاستقطاب وحشد الزعماء الأوروبيين في حملة الضغط التي شنها ضد الصين، التي كانت قد ابتدأت هجمات سيبرانية على الكثير من شركاتهم أيضا، لكن آماله تحطمت عندما كشفت وثائق سنودن أن وكالة الأمن القومي اخترقت ذات مرة الهاتف الجوال للمستشارة الألمانية أنجيلا ميركل Angela Merkel. كانت ميركل غاضبة ومستاءة[21].

هي أيضا، كان في امتعاضها واستشاطتها غضب أكثر من مجرد مسحة[22] من كابتن رينو؛ إذ إن «بي إن دي» BND، دائرة الاستخبارات الألمانية - مثلما كشفت تقارير إخبارية لاحقة - كانت دائمة التعاون مع وكالة الأمن القومي في رصد الجماعات الإرهابية المشتبه فيها. لكن في ذلك الوقت، لعبت ميركل جماهيريا، إذ إن قطاعا عريضا من الشعب الألماني، بما في ذلك الكثيرون ممن كانوا ذات مرة قد نظروا إلى أمريكا على أنها الحصن والصديق، بدأوا في تشبيه وكالة الأمن القومي بـ «شتازي» Stasi، وهي فرع المراقبة التدخلية المتطرفة للحكم الديكتاتوري الاستبدادي في ألمانيا الشرقية الذي جثم فترة طويلة. كشفت وثائق أخرى مما سربه سنودن عن

عمليات اعتراض كانت وكالة الأمن القومي تقوم بها في أمريكا الوسطى وأمريكا الجنوبية، مما أثار حنق الزعماء والمواطنين في النصف الغربي من الكرة الأرضية أيضا.

كان يتعين فعل شيء، كان ينبغي احتواء الرائحة الكريهة للنَتَن السياسي، والاقتصادي، والديبلوماسي. لذا فعل الرئيس أوباما ما كان قد فعله عديد من أسلافه في مواجهة الأزمات، إذ شكّل لجنة رفيعة المستوى «لجنة الوشاح الأزرق» blue-ribbon commission(*).

(*) لجنة الوشاح الأزرق blue-ribbon commission في الولايات المتحدة، هي مجموعة من الأشخاص الاستثنائيين المعينين للتحقيق في سؤال معين أو دراسته أو تحليله. عادة ما تتمتع لجنة الوشاح الأزرق بدرجة من الاستقلالية عن التأثير السياسي أو أي سلطة أخرى، وهي عادة لا تملك سلطة مباشرة خاصة بها. تأتي قيمة أعضاء اللجنة من قدرتهم على استخدام خبراتهم في إصدار النتائج أو التوصيات التي يمكن استخدامها من قبل أولئك الذين لديهم سلطة اتخاذ القرار للتصرف. [المترجم].

14

«تقرير الرفاق الخمسة»

«كان هذا يسمح لوكالة الأمن القومي بجمع وتخزين السجلات الخاصة بالاتصالات الهاتفية داخل الولايات المتحدة، وأرقام هواتف المتصلين، والتواريخ والتوقيتات والزمن الذي استغرقته المحادثات»

في 9 أغسطس من العام 2013، الذي صادف يوم جمعة حارا ورطبا، بُعيد الساعة الثالثة عصرا، أكثر الساعات كسلا في أشد شهور عاصمة البلاد كآبة ووحشة ليكون فيه أنباء، عقد الرئيس أوباما مؤتمرا صحافيا في القاعة الشرقية من البيت الأبيض؛ ليعلن أنه كان يعمل على تشكيل «مجموعة رفيعة المستوى[1] من الخبراء الخارجيين» لمراجعة ما تواجهه وكالة الأمن القومي من اتهامات بإساءة الاستخدام والتعسف في المراقبة.

قال: «إذا كنت خارج الأوساط الاستخباراتية، وإذا كنت شخصا عاديا، وبدأت ترى طائفة كبيرة من عناوين الأخبار تقول إن الأخ الأكبر

في الولايات المتحدة يستهتر بك وينظر إليك باستصغار، ويجمع سجلات الهاتف، وما إلى ذلك؛ حسنا، بطبيعة الحال، نتفهم أن الشعب كان سينتابه شعور بالقلق. أنا أيضا كنت سينتابني شعور بالقلق، إذا لم أكن داخل الحكومة». لكن أوباما كان داخل الحكومة، على قمتها، وكانت لديه ثقة بصلاح وكياسة الدوائر الحكومية. بالطبع، أقر أوباما: «بوصفي رئيسا، فإنه غير كاف بالنسبة إليَّ أن أكون مطمئنا إلى تلك البرامج. الشعب الأمريكي أيضا في حاجة إلى أن يكون مطمئنا إليها».

بدا كأنه كان يقول إن هذه ستكون هي مهمة هذه المجموعة رفيعة المستوى من الخبراء الخارجيين، إذ إن الغاية ليست أن توصي اللجنة بإصلاحات رئيسية مهمة، أو حتى إجراء تقصٍّ حازم وفعال ولا هوادة فيه؛ ولكن بدلا من ذلك، على حد تعبيره، «لبحث الكيفية التي نستطيع بها الحفاظ على ثقة الشعب». كان أوباما سيعمل أيضا مع الكونغرس من أجل «تحسين اطمئنان الشعب للدور الرقابي الذي تضطلع به محكمة مراقبة الاستخبارات الأجنبية». تلك الجهود «كانت مخصصة لضمان أن الشعب الأمريكي يستطيع أن يثق بي» إن أعمال دوائر الاستخبارات كانت «تتسق مع مصالحنا وقيمنا». ربما تطرح المجموعة رفيعة المستوى، أو اللجان المختارة من الكونغرس المعنية بالاستخبارات، أساليب لـ «الخضخضة الطفيفة» من أجل التوازن بين الأمن القومي والخصوصية، الذي كان لا بأس به. قال أوباما: «إذا كانت هناك أمور إضافية نستطيع القيام بها لإعادة بناء تلك الثقة، فإنه لزاما علينا القيام بها». لكنه بدا أنه يفترض أن التغييرات الكبيرة ستكون غير ضرورية. وقال: «في الوقت الحالي، أشعر بالارتياح إلى أنه لا يُساء استخدام البرنامج. السؤال هو: كيف أجعل الشعب الأمريكي أكثر ارتياحا؟».

في ذلك اليوم نفسه[2]، كأنه كان من أجل ختم القضية وإغلاقها، نشرت إدارة أوباما «ورقة بيضاء» white paper(*) تتألف من ثلاث وعشرين صفحة، تبين الذريعة القانونية للتجميع الضخم للبيانات الواصفة من الاتصالات الهاتفية للأمريكيين، وأصدرت وكالة الأمن القومي - في سبع صفحات - مذكرتها التوضيحية الخاصة بها، شارحة غرض البرنامج ومحدداته.

(*) ورقة بيضاء white paper: هي وثيقة رسمية تطرح فلسفة المؤسسة التي أصدرتها، وتبين توجهاتها وسياساتها، وقد يكون أول استخدام لهذه العبارة في العام 1922، عندما أصدر «وينستون تشيرشل» ورقة بيضاء بشأن اتصالاته مع العرب واليهود بخصوص فلسطين. [المترجم].

وبحلول ذلك الوقت، كان أوباما وكبير موظفي البيت الأبيض «دنيس ماكدونو» Denis McDonough، و«سوزان رايس» Susan Rice، التي كانت سفيرة الولايات المتحدة في الأمم المتحدة، في أثناء فترة رئاسته الأولى، والتي حلت أخيرا محل «توم دونيلون» مستشارا للأمن القومي، بالفعل قد فكروا مليا في المرشحين المحتملين لفريق الخبراء الخارجيين. قبل بضعة أيام من المؤتمر الصحافي، اختاروا خمسة أشخاص، وطلبوا منهم الانضمام إلى المجموعة، وبعد الحصول على قبولهم المهمةَ، أمر مكتب التحقيقات الفدرالي أن يسرع في مراجعة تراخيصهم الأمنية.

لم تكن المجموعة برمتها خارجية أو مستقلة. كان جميع أعضائها الخمسة أصدقاء قدامى، أو معاونين سابقين للرئيس أوباما. مع ذلك، كانوا ثلة متباينة تأسر اللب ومُثيرة للاهتمام على نحو يفوق ما توقعه المتشككون إثر مؤتمره الصحافي.

كان «مايكل موريل» Michael Morell هو خيرة التشكيل، ومن الخبراء المحنكين في وكالة الاستخبارات المركزية لمدة ثلاثة وثلاثين عاما، وكان قد تقاعد قبل شهرين من منصب نائب مدير الوكالة، وكان هو نقطة الاتصال الرئيسية بين «لانغلي» والبيت الأبيض في أثناء الغارة السرية على مخبأ «أسامة بن لادن» في «باكستان». إن وجود موريل في المجموعة كان سيسهم في تقريب المسافة نحو استرضاء الأوساط الاستخباراتية.

كان اثنان من الخيارات تزاملا مع أوباما منذ أن كان يدرِّس في مدرسة القانون بجامعة شيكاغو، في التسعينيات من القرن العشرين. كان أحدهما هو «كاس صنشتاين» Cass Sunstein الذي عمل أيضا في حملة أوباما الرئاسية، وعمل ثلاثة أعوام مديرا إداريا لمكتبه الرقابي، وكان متزوجا من «سامانتا باور» Samantha Power التي كانت على مدى فترة طويلة معاونة أوباما للسياسة الخارجية، والتي حلت أخيرا محل سوزان رايس سفيرة في الأمم المتحدة. إن صنشتاين مفكر غير نمطي في قضايا متفاوتة تشمل التعديل الأول لدستور الولايات المتحدة الأمريكية المتعلق بحقوق الحيوان، وكان قد كتب بحثا أكاديميا في العام 2008[3]، مقترحا أن تندس دوائر الحكومة في الشبكات الاجتماعية للجماعات المتطرفة، وتنشر رسائل لتقويض نظريات المؤامرة لديهم. أخذ بعض

منتقدي فريق أوباما هذا البحث على أنه إشارة إلى أن صنشتاين كان ميالا إلى ما تقوم به وكالة الأمن القومي من مراقبة داخلية.

كان الآخر أيضا من ولاية شيكاغو، وهو «جيوفري ستون» Geoffrey Stone[4]، وكان عميدا لمدرسة القانون، حينما كان أوباما يدرِّس هناك. وهو عضو بارز في «المجلس الاستشاري الوطني للاتحاد الأمريكي للحريات المدنية»، ومؤلف لكتب مرموقة حظيت بإشادة كبيرة حول التعديل الأول لدستور الولايات المتحدة الأمريكية في زمن الحرب، وعن التكتم المفرط لمؤسسة الأمن القومي، بدا أن «ستون» هو منتقد مرجح لتجاوزات وكالة الأمن القومي.

كان «بيتر سواير» Peter Swire[5]، أستاذ القانون في «معهد جورجيا للتكنولوجيا»، منذ فترة طويلة مناصرا قديما للخصوصية على الإنترنت، وكاتبا لمقال بارز يمثل نقطة تحول بشأن قانون المراقبة. بصفته مستشار البيت الأبيض لشؤون الخصوصية في أثناء فترة رئاسة «بيل كلينتون»، كان سواير يؤدي دورا رئيسيا في الجدال الذي دار حول «رقاقة كليبر»، يسوق الحجج ضد محاولة وكالة الأمن القومي وضع مراقبة على التشفير التجاري، التي كان - على نحو صائب - يرى أنها عقيمة ولا طائل منها. بعد مضي نحو عامين، وأيضا على أرضية الخصوصية، أقام سواير الحجة والدليل ضد خطة «ريتشارد كلارك» المشؤومة لوضع صناعات البنية الأساسية الحرجة على شبكة إنترنت منفصلة وربطهما سلكيا معا، حيث إنه كان سيجري تنبيه مكتب التحقيقات الفدرالي مباشرة في حالة حدوث خرق أمني.

لهذا السبب، كان سواير منفعلا حينما علم أن العضو الخامس في مجموعة المراجعة سيكون ريتشارد كلارك ذاته، المسؤول السابق في البيت الأبيض الذي كان قد انغمس في ممارسات وكالة الأمن القومي، كاتبا لتوجيهات رئاسية بشأن الأمن السيبراني، واكتسب شهرة أنه متعنت شديد البأس لا يلين في الترويج لوجهات نظره الخاصة، وسحق وجهات نظر الآخرين. بصورة عامة، كان ينظر إلى كلارك على أنه ورقة رابحة.

كان كلارك لايزال مديرا من الطراز الأول وشديد البراعة، وقد حقق نجاحا باهرا وحصد كثيرا من الاهتمام العام منذ أن ترك البيت الأبيض في عهد بوش عشية حرب العراق. بعد مضي عام واحد على الغزو، اكتسب شهرة لا تصدق باعتباره بطلا شعبيا أمريكيا في جلسات استماع لجنة الحادي عشر من سبتمبر التي كانت تُبث

على التلفاز الوطني، مفتتحا شهادته باعتذار. بدأ كلارك: «إلى أحباء ضحايا[6] أحداث 11 سبتمبر، إلى هؤلاء الذين هنا في هذه القاعة، إلى أولئك الذين يشاهدون على التلفاز. إن حكومتكم خذلتكم، خذلكم أولئك المناط بهم حمايتكم، وأنا خذلتكم. نحن حاولنا جاهدين، لكن هذا لا يهم، لأننا فشلنا، وبسبب هذا الفشل، أنا كنت سألتمس منكم تفهمكم وصفحكم، حالما تظهر كل الحقائق».

بدا الأمر كأنه اعتراف بالذنب صادق، وبندم عميق، معززا بحقيقة أنه لم يكن أي مسؤول رسمي آخر في عهد بوش، في الماضي أو الحاضر، قد اعتذر بشأن أي شيء؛ واهتزت جنبات القاعة بعاصفة مدوية من التصفيق له. بعد إدلائه بشهادته، اصطف أفراد عائلات الضحايا لشكره، ومصافحته، وعناقه.

الجمع الغفير من منتقدي كلارك تهكم من أنه كان يسعى إلى الشهرة والدعاية فقط. كان كتابه الجديد «ضد كل الأعداء.. داخل حرب أمريكا على الإرهاب» Against All Enemies: Inside America's War on Terror قد حقق نجاحا يوم الجمعة الذي سبق، وجرى الترويج له في إحدى فقرات البرنامج التلفزيوني الإخباري «60 دقيقة» 60 Minutes[7] الذي كان يعرض على قناة «سي بي إس» التلفزيونية ليلة يوم الأحد بين تاريخ صدوره وجلسة الاستماع. حينما قفز الكتاب إلى صدارة قائمة الكتب الأفضل مبيعا، اعترض منتقدوه على مزاعمه بأنه في الأشهر التي سبقت الحادي عشر من سبتمبر، كان كبار المسؤولين في عهد بوش يتجاهلون التحذيرات (بما في ذلك تحذيرات كلارك) من هجوم وشيك يقوم به تنظيم القاعدة؛ إذ إنه في اليوم التالي لسقوط البرجين التوأمين، ضغط بوش ذاته على كلارك ودفعه إلى إيجاد دليل ليلقي باللوم على صدام حسين لتبرير الحرب المقبلة على العراق. لكن كلارك الذي كان دائما مقاتلا بيروقراطيا مشاكسا، لم يكن قط ليعرض نفسه لمثل هذه اللطمة السهلة، كان يعرف أن الوثائق ستدعمه وتحميه، وهكذا فعلت حينما كانت تفد شيئا فشيئا إلى ضوء النهار لتتكشف وتتضح.

على الرغم من ذلك، استبقى كلارك على الدوام شغفه بالقضايا السيبرانية، وبعد مضي ستة أعوام، كتب كتابا بعنوان «الحرب السيبرانية.. التهديد التالي للأمن القومي وماذا نفعل حياله» Cyber War: The Next Threat to National Security and What to Do About It. نُشر الكتاب في أبريل من العام 2010[8]، وقد

استاء منه كثيرون باعتباره طنانا ومبالغا فيه، على نحو مشروع في بعض التفاصيل (نسب إلى الهجمات السيبرانية أنها كانت هي السبب المحتمل لبضع حالات انقطاع الكهرباء الرئيسية التي شُخِّصت على نحو مقنع على أنها حوادث شاذة أو حوادث صيانة مؤسفة)، ولكن على نحو مجحف وجائر بالمفهوم الواسع للأمور. رأى بعض النقاد - لاسيما أولئك الذين كانوا يعرفون المؤلف - أن الكتاب ما هو إلا تباهٍ وتضخيم للذات، إذ إن كلارك كان وقتها رئيسا لشركة متخصصة في إدارة الأخطار السيبرانية تسمى «جوود هاربر» Good Harbor، ومن ثم رأوا كتاب «الحرب السيبرانية» على أنه كتيب دعائي لترويج الأعمال.

لكن السبب الرئيسي لرد الفعل الرافض هو أن سيناريوهات الكتاب وتحذيراته بدت مستبعدة جدا، وضربا من ضروب الخيال العلمي. كانت افتتاحية مقال «إطرائي بوجه عام» لاستعراض الكتاب نشر في صحيفة «واشنطن بوست» The Washington Post قد عبرت عن الارتياب على نحو هزلي ساخر: «الحرب السيبرانية، هذا السيبراني[9]، ذاك السيبراني: ماذا بشأن الكلمة التي تجعل العيون تدور وتنقلب إلى أعلى من شدة السخط ونفاد الصبر؟ كيف يمكن للحرب أن تكون أصيلة وذات حجية حينما لا تكون هناك أشياء تنفجر؟

كان قد مضى أكثر من أربعين عاما على البحث الذي كان «ويليس وير» قد أعده بشأن ضعف شبكات الحاسوب وثغراتها الأمنية، ونحو ثلاثين عاما منذ صدور التوجيه الرئاسي السري المتعلق بالأمن القومي (إن إس دي دي - 145» NSDD-145 الذي أصدره «رونالد ريغان»، وأكثر من عقد منذ تدريب «المتلقي المؤهل»، وتقرير «مارش»، وتحقيقات «الشروق الشمسي» (سولار صانرايز) ، وعملية «متاهة ضوء القمر» (موونلايت ميز)، تلك الأحداث التي تعد المحك والمرجعية في حياة من هم منغمسون في الفضاء السيبراني؛ لكن، تقريبا لكل شخص آخر، فقد طواها النسيان، إن كانت في الأساس معروفة. حتى «اختبار المولد الكهربائي أورورا»، الذي جرى قبل ذلك بستة أعوام فقط، والعمليات السيبرانية الهجومية في سورية، وأستونيا، وأوسيتيا الجنوبية، والعراق، التي كانت لاتزال تجرى في الآونة الأخيرة، لم يكن لها تأثير ذو شأن في الوعي العام.

ليس إلا بعد بضعة أعوام من كتاب كلارك، مع انكشاف عملية «ستوكسنت»، وتقرير «مانديانت» بشأن الوحدة الصينية الرقم 61398، وأخيرا ما فعله «إدوارد

سنودن» من تسريب هائل لوثائق وكالة الأمن القومي، صار التجسس السيبراني والحرب السيبرانية مادتين للأخبار الرئيسية والمحادثة اليومية. كانت السيبرانية تتصاعد وتعتلي القمة على نحو مفاجئ، وحينما استجاب أوباما للجلبة بتشكيل لجنة رئاسية، كان من الطبيعي أن يكون كلارك، الذي يجسد الصورة الرمزية لرهاب السيبرانية، من بين المعينين فيها.

في 27 أغسطس[10]، اجتمع أعضاء اللجنة الخمسة في غرفة العمليات بالبيت الأبيض مع الرئيس، وسوزان رايس، ورؤساء دوائر الاستخبارات، وفي اليوم نفسه جرى الاحتفاء بهم، وتسمية اللجنة على أنها مجموعة الرئيس لإعادة النظر في الاستخبارات وتكنولوجيا الاتصالات. كانت الجلسة قصيرة، حدد أوباما لأعضاء المجموعة موعدا نهائيا لتقريرهم هو يوم 15 ديسمبر، وأكد لهم أنه سيتاح لهم إمكان الوصول إلى أي شيء يريدونه. كان ثلاثة من أعضاء اللجنة من المحامين، لذا أوضح أوباما أنه لا يريد تحليلا قانونيا؛ وقال: نفترض أننا نستطيع الاضطلاع بهذا النوع من المراقبة على أسس قانونية، مهمتكم هي أن تخبروني ما إذا كان ينبغي لنا الاضطلاع بذلك كسياسة، وإذا لم يكن كذلك، فعليكم أن تتوصلوا إلى شيء أفضل.

أضاف أوباما أنه كان يميل إلى اتباع أي اقتراحات يقدمونها، مع تحفظ واحد هو أنه لم يكن ليقبل أي اقتراح ربما يعوق قدرته على وقف هجوم إرهابي.

على مدار الأشهر الأربعة اللاحقة، كانت المجموعة تجتمع يومين في الأسبوع على الأقل، وأحيانا تصل إلى أربعة أيام، وعادة مدة اثنتي عشرة ساعة أو أكثر في اليوم، يجرون مقابلات مع المسؤولين، ويحضرون جلسات إحاطة، ويفحصون الوثائق، ويناقشون التداعيات والآثار المترتبة.

في اليوم الأول، قبل جلستهم مع الرئيس، بوقت قصير، التقى الخمسة معا في الجناح المكتبي الذي جرى استئجاره لاستخدامهم، وكان بعضهم يتقابل للمرة الأولى. كانت خطتهم المبدئية هي العمل داخل مقر مدير الاستخبارات القومية في «تايسونز كورنر» Corner بولاية فرجينيا، قبالة «بيلتواي» Beltway، على مسافة عشرة أميال من وسط مدينة واشنطن. لكن كلارك اقترح أن يستخدموا أحد مواقع «سكيف» SCIF الأكثر قربا - «سكيف» هي «منشأة مجتزأة للمعلومات الحساسة» Sensitive Compartmented Information Facility (SCIF)، تجري حراستها

على نحو احترافي وذات بنية محصَّنة لمنع المتسللين من سرقة الوثائق أو التنصت على المحادثات، سواء بالأساليب الإلكترونية أو خلافه. على وجه الخصوص، أشار كلارك إلى أحد مواقع «سكيف» SCIF الذي يقع في شارع كيه K Street، كان ذلك الموقع سيبقي أعضاء اللجنة على بُعد بضع بنايات من البيت الأبيض، وكان سيحافظ على استقلاليتهم عن الأوساط الاستخباراتية، ماديا وخلاف ذلك. لكن دافع كلارك الحقيقي، الذي أدركه زملاؤه في وقت لاحق، كان هو أن موقع «سكيف» SCIF هذا كان يقع في الجهة المقابلة لمكتب شركته الاستشارية، فضّل كلارك عدم القيادة إلى الضواحي كل يوم وسط الزحام المروري في غمرة ساعة الذروة الكثيفة.

في ذلك اليوم الأول داخل موقع «سكيف» SCIF، التقوا أيضا مع ضباط الاستخبارات التسعة المعارين من مختلف الدوائر، الذين كانوا سيخدمون في المجموعة باعتبارهم موظفين. وكما أوضح أحدهم، كان الموظفون سيمارسون العمل الإداري من ترتيب مواعيد المجموعة، وتنظيم ملاحظاتها، وكتابة التقرير في النهاية، تحت توجيه المجموعة بطبيعة الحال.

نظر أعضاء مجموعة المراجعة بعضهم إلى بعض وابتسموا، وضحك عدد منهم. كان أربعة منهم - كلارك، وستون، وصنشتاين، وسواير - منهم من كتب ما يربو على الستين كتابا، وهم كانوا عاقدي العزم على كتابة هذا أيضا. لم تكن هذه اللجنة في سبيلها إلى أن تكون مثل اللجان الرئاسية المعتادة.

في صباح اليوم التالي[11]، أُقِلُّوا إلى «فورت ميد». لم يكن أي منهم قد دخل المكان من قبل سوى كلارك ومورل. كانت وجهة نظر كلارك بشأن الوكالة أكثر تشككا مما كان البعض يفترض. كان كلارك في كتابه «الحرب السيبرانية» قد انتقد[12] اندماج وكالة الأمن القومي والقيادة السيبرانية تحت قيادة جنرال واحد من فئة النجوم الأربعة، خوفا من أن تضع هذه الفعلة كثيرا من السلطة في يدي شخص واحد، وتفرط في التركيز على العمليات الهجومية السيبرانية، على حساب الأمن السيبراني للبنية الأساسية الحرجة.

كان سواير، فقيه الخصوصية على الإنترنت، قد تعامل مع ضباط وكالة الأمن القومي في أثناء جدال «رقاقة كليبر»، وكان يتذكرهم كأذكياء ومهنيين، ولكن ذلك كان قبل خمسة عشر عاما؛ ولم يكن يعرف ما الذي يتوقعه في الوقت الحالي. من دراسته

محكمة قانون مراقبة الاستخبارات الأجنبية، عرف بشأن القرارات الصادرة التي سمحت لوكالة الأمن القومي باستدعاء سلطاتها للاستخبارات الأجنبية لرصد المكالمات الهاتفية المحلية؛ لكن أدهشه ما أشارت إليه وثائق إدوارد سنودن من أن الوكالة كانت تستخدم صلاحياتها ذريعة لجمع كل المكالمات. إذا كان هذا صحيحا، فقد كان الأمر تجاوزا صارخا للحدود. كان لدى سواير فضول لسماع رد وكالة الأمن القومي.

ستون، المحامي الدستوري وأحد أعضاء المجموعة الذين لم يسبق لهم قط الاتصال بعالم الاستخبارات، كان يتوقع أن يجد وكالة مارقة. لم يكن سنودن يروق له[13]، إذ إنه كان يقدر بعض كاشفي الفساد ممن يسربون الأسرار على نحو انتقائي من أجل المصلحة العامة؛ لكن ما فعله سنودن من سرقة بالجملة لعدد كبير من الوثائق التي لها مثل هذه الطبيعة شديدة السرية، يعصف به فيما يتعذر الدفاع عنه. ربما كان سنودن على حق، وكانت الحكومة على خطأ - لم يكن ستون يعرف - لكنه اعتقد أنه لا يوجد جهاز أمن قومي يستطيع أن يؤدي وظيفته إذا قرر أحد صغار الموظفين ما هي الأسرار التي تُحفظ، وأي منها يسمح بإطلاقها. مع ذلك، هالته وروَّعته الأسرار التي ظهرت حتى الآن بما كشفته عن مدى اتساع نطاق المراقبة المحلية. كان ستون قد ألَّف كتابا حصل على جائزة، تناول الكتاب ميل حكومة الولايات المتحدة عبر التاريخ إلى المبالغة في ردة الفعل في مواجهة تهديدات الأمن القومي، من «القانون المتعلق بإثارة الفتنة» Sedition Act إلى «حقبة ماكارثي» McCarthy era، إلى مراقبة الناشطين المناهضين لحرب فيتنام. وأشارت بعض وثائق سنودن إلى أن رد الفعل على أحداث 11 سبتمبر ربما يكون مثالا آخر على ذلك. كان ستون بالفعل يفكر مليا في سبل لتشديد الضوابط والتوازنات الرقابية.

عند وصولهم إلى «فورت ميد»، أُخذوا إلى قاعة اجتماعات واستقبلهم ستة من كبار مسؤولي وكالة الأمن القومي، من بينهم الجنرال ألكسندر ونائبه، وجون سي كريس إنجليس John C. «Chris» Inglis. كان إنجليس، الطيار السابق في سلاح الجو والحاصل على درجات علمية عليا في علوم الحاسوب، قد أمضى فترة شبابه كاملة في الوكالة، سواء في الملحق الدفاعي، أو في عمليات استخبارات الإشارة (سيجينت). وكان من بين عشرات عدة من الشباب اللامع الذين رقّاهم كين مينيهان ومايك هايدن مبكرا كجزء من إصلاحات الوكالة بعد الحرب الباردة.

بعد بعض الملاحظات الافتتاحية، أوجد ألكسندر لنفسه مخرجا، وخلال اليوم كان يعود إلى الاجتماع على نحو دوري، تاركا إنجليس يتولى زمام الأمور. على مدار الساعات الخمس اللاحقة، قدم إنجليس ومسؤولون آخرون تقارير موجزة بشأن برامج المراقبة محل الخلاف، وخاضوا بعمق في التفاصيل.

كان أكثر البرامج إثارة للجدل هو ما كان يتم من تجميع ضخم بالجملة للبيانات الواصفة للاتصالات الهاتفية، على النحو المأذون به بموجب المادة 215 من قانون مكافحة الإرهاب Patriot Act. وفقا لوثائق سنودن، كان هذا يسمح لوكالة الأمن القومي بجمع وتخزين جميع السجلات الخاصة بالاتصالات الهاتفية داخل الولايات المتحدة، ليس محتويات تلك الاتصالات، ولكن أرقام هواتف المتصلين، بالإضافة إلى التواريخ والتوقيتات والزمن الذي استغرقته المحادثات، والتي في حد ذاتها كان يمكن أن تكشف كثيرا من المعلومات.

أخبر إنجليس المجموعة بأن هذه لم تكن في الواقع هي الكيفية التي كان يُشغل البرنامج بها فعليا. في القرار الصادر عن محكمة قانون مراقبة الاستخبارات الأجنبية بشأن المادة 215، كانت وكالة الأمن القومي تستطيع الخوض في هذه البيانات الواصفة، بحثا عن علاقات وارتباطات بين أرقام الهاتف المختلفة، فقط بغرض العثور على مشاركين من ثلاث منظمات إرهابية أجنبية محددة، منها تنظيم «القاعدة».

قاطعه كلارك قائلا: لقد تكبدت كل هذه المشقة لإعداد هذا البرنامج، وأنت تبحث عن علاقات وارتباطات لثلاث منظمات فقط؟

أجاب إنجليس: هذا كل ما لدينا من سلطة للقيام به. علاوة على ذلك، إذا كشفت البيانات الواصفة[14] أن أحد الأشخاص داخل الولايات المتحدة قد اتصل مع - أو اتصل به - أحد الإرهابيين المشتبه فيهم، فإن اثنين وعشرين شخصا فقط في وكالة الأمن القومي برمتها - عشرين من موظفي الخطوط واثنين من المشرفين - كانوا هم القادرين على طلب وفحص مزيد من البيانات بشأن ذلك الرقم الهاتفي. وقبل أن يمكن تقصي تلك البيانات، كان يتعين موافقة اثنين من أولئك الأفراد العشرين وواحد على الأقل من المشرفين كل على حدة، على أن البحث الموسع كان جديرا بالاهتمام وذا منفعة. في النهاية، كانت صلاحية البحث في سجلات الهاتف الخاصة بذلك الشخص ستنتهي بعد 180 يوما.

إذا ظهر شيء مريب في أحد تلك الأرقام، كان في إمكان محللي وكالة الأمن القومي القيام بقفزة ثانية؛ بعبارة أخرى، كان في استطاعتهم استخلاص قائمة بجميع الاتصالات التي كانت تلك الأرقام قد أجرتها، والتي استقبلتها. لكن إذا رغب المحللون في توسيع نطاق البحث إلى قفزة ثالثة للنظر في الأرقام التي اتصلت بها أو استقبلتها تلك الهواتف، كان سيتعين عليهم المضي في الإجراءات نفسها مجددا، والحصول على إذن من المشرف ومن المستشار العام لوكالة الأمن القومي (كان المحللون عادة يتخذون قفزة ثانية[15]، لكنهم تقريبا لم يتخذوا قط قفزة ثالثة).

من النظرات التي تبادلوها عبر الطاولة، بدا جميع أعضاء مجموعة المراجعة الخمسة مقتنعين بأن برنامج المادة 215 كان صارما ومحترما (بافتراض أن هذا الجزء من الإحاطة قد تأكد في تقصي ملفات الوكالة)، إذ إنه كان بإذن من الكونغرس، ووافقت عليه محكمة قانون مراقبة الاستخبارات الأجنبية، ومحدود النطاق، ويُرْصَد على نحو أكثر صرامة مما كان أي منهم قد تخيل. لكن الرئيس أوباما كان قد أخبرهم بأنه لا يريد رأيا قانونيا في البرامج، كان يريد تقديرا عاما بشأن ما إذا كانت جديرة بالاهتمام وذات منفعة.

لذا سأل الأعضاء عن نتائج هذه المراقبة، كم عدد المرات التي كانت وكالة الأمن القومي قد استعلمت فيها قاعدة البيانات، وكم عدد المؤامرات الإرهابية التي أُحبطت نتيجة لذلك؟

أحد كبار المسؤولين الآخرين كانت لديه أرقام دقيقة في متناول يده. طوال العام 2012 بكامله[16]، استعلمت وكالة الأمن القومي من قاعدة البيانات الخاصة عن 288 رقم هاتف بالولايات المتحدة. نتيجة لتلك الاستعلامات، مررت الوكالة اثني عشر «تلميحا» tip إلى مكتب التحقيقات الفدرالي. إذا وجد مكتب التحقيقات الفدرالي التلميحات مثيرة للاهتمام، فإنه كان يمكنه طلب إذن قضائي من المحكمة لاعتراض الاتصالات من وإلى هذا الرقم الهاتفي - للتنصت على المكالمات - باستخدام تكنولوجيا وكالة الأمن القومي، إذا لزم الأمر.

ثم سأل أحد المفوضين أعضاء اللجنة: كم من هذه التلميحات الاثني عشر أدى إلى وقف مؤامرة أو اصطياد أحد الإرهابيين؟

كان الجواب صفرا. لم يكن أي من التلميحات قد أدى إلى أي شيء يستحق مزيدا من المتابعة، لم تكن أي من حالات الاشتباه قد حققت نجاحا.

صعق جيوفري ستون، وجال بفكره: «آه، مرحبا[17]، ما الذي نفعله هنا؟» برنامج البيانات الواصفة الذي كثر الحديث عنه ويتباهون به: (أ) بدا أنه يخضع لرقابة صارمة، (ب) لم يتتبع كل اتصال هاتفي في أمريكا، والآن اتضح أنه، (ج) لم يكن قد كشف عن إرهابي واحد.

طرح كلارك السؤال الخفي، لماذا لايزال لديك هذا البرنامج إذا لم يكن قد أسفر عن أي نتائج؟

أجاب إنجليس بأن البرنامج عجَّل من عملية قبض مكتب التحقيقات الفدرالي على إرهابي واحد على الأقل. وأضاف أنه ربما يشير إلى مؤامرة في وقت ما في المستقبل. في نهاية المطاف، البيانات الواصفة موجودة. وتجمعها شركات الهاتف على نحو اعتيادي على أنها سجلات عمل، وكانت ستستمر في القيام بذلك، مع أو من دون وكالة الأمن القومي أو المادة 215. بما أنها هناك، فلماذا لا تُستخدم؟ إذا اتصل أحد الأشخاص في الولايات المتحدة هاتفيا بأحد الإرهابيين المعروفين، ألم يكن من المحتمل أن هناك مؤامرة تُحاك؟ مادامت قد اتُّخذت ضمانات ملائمة لحماية خصوصية الأمريكيين، فلماذا لا ننظر في الأمر؟

ظل المتشككون غير مقتنعين من حيث المبدأ. كان هذا أمرا تلزم دراسته بمزيد من التعمق.

انتقل إنجليس إلى ما كان يعتبره هو وزملاؤه أنه أكثر تسريبات سنودن أهمية وإضرارا. إنه التسريب المعني بالبرنامج المعروف باسم «بريزم» PRISM[18]، والذي فيه تجسست وكالة الأمن القومي ومكتب التحقيقات الفدرالي على المخدمات المركزية لتسع من شركات الإنترنت الأمريكية الرائدة؛ بصفة رئيسية «مايكروسوفت» Microsoft، و«ياهو» Yahoo، و«غوغل» Google، ولكن أيضا «فيسبوك» Facebook، و«أمريكا أونلاين» AOL، و«سكايب» Skype، و«يوتيوب» YouTube، و«بل» Apple، و«بالتوك» Paltalk؛ لاستخلاص رسائل البريد الإلكتروني، والوثائق، والصور، وملفات الصوت والفيديو، وسجلات الاتصال. أفادت التقارير الإخبارية حول برنامج «بريزم»، بأن الغرض من الاعتراضات كان يقتصر على تتبع

الأهداف الأجنبية، لكن التقارير أشارت أيضا إلى أنه في أثناء هذه العملية، كان يجري تفحص والتقاط رسائل البريد الإلكتروني ومكالمات الهاتف الجوال لعامة الأمريكيين أيضا.

كانت وكالة الأمن القومي قد أصدرت بيانا فور ظهور أول التقارير الإخبارية، واصفة «بريزم» بأنه «الأداة الأبرز[19] في ترسانة وكالة الأمن القومي للكشف عن، وتحديد، وعرقلة التهديدات الإرهابية للولايات المتحدة وحول العالم». كان الجنرال ألكسندر قد صرح علنا[20] بأن البيانات التي جُمعت من «بريزم» ساعدت على اكتشاف وعرقلة التخطيط لأربعة وخمسين هجوما إرهابيا، وهو ادعاء كان إنجليس يكرره أمام المجموعة، عارضا تشارك جميع ملفات القضية معها.

أضاف أنه مهما كان الغموض الذي يكتنف برنامج البيانات الواصفة الهاتفية، فإنه يمكن الإثبات بالدليل الدامغ أن «بريزم» قد أنقذ أرواحا.

هل كانت تُلتقط في أثناء عملية المسح الاتصالات الهاتفية ورسائل البريد الإلكتروني الخاصة بالأمريكيين؟ نعم، لكن هذا كان ناتجا عرضيا للتكنولوجيا وحتميا ولا يمكن تفاديه. بالنسبة إلى أي شخص كان سيستمع، فإن مقدمي الإحاطات من وكالة الأمن القومي كانوا يشرحون لمجموعة المراجعة ما كان مايك ماكونيل قد شرحه من قبل في العام 2007، وهو أن الاتصالات الرقمية تتحرك في حزم، متدفقة عبر المسار الأكثر كفاءة، ولأن معظم النطاق الترددي للعالم كان يتركز في الولايات المتحدة، فإن بعضا - تقريبا - من كل رسالة بريد إلكتروني ومحادثة هاتف جوال في العالم، عند نقطة ما، كانت تتدفق عبر خط من الألياف الضوئية المتموضعة في أمريكا.

في عصر الخطوط الأرضية والبث بالموجات الميكروية، كان إذا اتصل هاتفيا أحد الإرهابيين في باكستان بإرهابي آخر في اليمن، كانت وكالة الأمن القومي تستطيع اعتراض محادثتهما من دون تقييد. على الرغم من ذلك، في الوقت الحالي إذا تحدث الشخصان أنفسهما، في المواضع الخارجية ذاتها، عبر الهاتف الجوال، وأراد محللو وكالة الأمن القومي الإمساك بحزمة تحتوي على جزء من تلك المحادثة في أثناء تدفقها داخل الولايات المتحدة، فسيكون لزاما عليهم الحصول على إذن من محكمة مراقبة الاستخبارات الأجنبية. إنه أمر غير منطقي.

لهذا السبب كان ماكونيل يجاهد من أجل إعادة النظر في القانون، وهذا هو ما أدى إلى سن قانون حماية أمريكا Protect America Act للعام 2007، وقانون مراقبة الاستخبارات الأجنبية المعدل FISA Amended Act للعام 2008، وبخاصة المادة 702 التي كانت تسمح للحكومة بإجراء مراقبة إلكترونية داخل الولايات المتحدة بـ «مساعدة مزود خدمة اتصالات» - وفق تعبير ذلك القانون - مادام الأشخاص الذين يتواصلون كانوا «يعتقد على نحو معقول» خارج الولايات المتحدة.

كانت شركات الإنترنت التسع، التي ذُكر اسمها في التقارير الإخبارية، إما قد امتثلت لطلبات وكالة الأمن القومي للتنصت على مخدماتها، وإما أنها كانت قد تلقت أمرا من محكمة قانون مراقبة الاستخبارات الأجنبية للسماح لوكالة الأمن القومي بالدخول. وفي كلتا الحالتين، كانت الشركات قد عرفت منذ فترة طويلة ما الذي كان يجري.

كان قدر كبير من هذا جليا لمجموعة المراجعة، لكن بعض الإجراءات التي وصفها إنجليس والآخرون كانت مربكة. ماذا يعني أن المتصلين هاتفيا «يُعتقد على نحو معقول» أنهم على أرض أجنبية؟ كيف كان يُجري محللو وكالة الأمن القومي هذا التقييم؟

استعرض مقدمو الإحاطات قائمة من «المحددات» التي كانت تشير إلى احتمال أن يكون «أجنبيا»، وهي عمليات بحث باستخدام كلمات مفتاحية وغيرها من علامات التمييز، ومع فحص المزيد من المحددات، كان الاحتمال يتزايد. كان من الممكن أن يبدأ الاعتراض بصورة قانونية مشروعة حالما كان هناك احتمال بنسبة 52 في المائة[21] أن يكون طرفا الاتصال الهاتفي أو البريد الإلكتروني مقيمين في الخارج.

علق بعض أعضاء مجموعة المراجعة بأن هذا الأمر كان يبدو كأنه عملية حسابية متقلبة ومشكوك بها، وفي جميع الأحوال، فإن 52 في المائة كانت تمثل حدا منخفضا جدا. سلم مقدمو الإحاطة بهذه النقطة. لذلك، أضافوا، حالما يبدأ الاعتراض، إذا تبين أن الأطراف كانوا داخل الولايات المتحدة كان يتعين إيقاف العملية على الفور، وكان ينبغي تدمير كل البيانات التي استُرجعت حتى اللحظة.

أيضا أشار مقدمو الإحاطة إلى أنه على الرغم من أن إذن المحكمة لم يكن إلزاميا في تلك الاعتراضات المستندة إلى المادة 702، فإن وكالة الأمن القومي لم تكن

تستطيع اصطياد أي شيء. في كل عام كان يتعين تصديق مدير الوكالة[22] والمدعي العام للولايات المتحدة على قائمة تحدد فئات الأهداف الاستخباراتية التي كان يمكن اعتراضها تحت المادة 702 وتوافق على القائمة محكمة قانون مراقبة الاستخبارات الأجنبية. ثم، كل خمسة عشر يوما، بعد بدء اعتراض جديد، كانت لجنة خاصة داخل وزارة العدل تراجع العملية وتتأكد من مطابقتها تلك القائمة. وأخيرا، كل ستة أشهر، كان النائب العام يستعرض ويراجع كل الاعتراضات التي بدأت، ويقدمها إلى لجان الكونغرس المعنية بالاستخبارات.

لكن كانت هناك مشكلة في كل هذا. للوصول إلى هدف الرصد كان يتعين على رجال العمليات في وكالة الأمن القومي اغتراف وتفحص الحزمة بكاملها التي كانت تحمل الاتصال المعني. كانت هذه الحزمة تتشابك مجدولة مع حزم أخرى بالقطع تحمل أجزاء من اتصالات أخرى، ولا شك أن كثيرا منها يتضمن أمريكيين. ماذا كان يحدث لكل تلك الأجزاء؟ كيف كانت الوكالة تتأكد من عدم قراءة بعض المحللين لتلك الرسائل الإلكترونية، أو الاستماع إلى تلك المحادثات على الهواتف الجوالة؟

أثار مقدمو الإحاطات تلك الأسئلة بأنفسهم، لأنه، قبل ذلك بأسبوع واحد فقط، كان الرئيس أوباما قد رفع الحظر عن قرار أصدره قاض في محكمة قانون مراقبة الاستخبارات الأجنبية يدعى جون بيتس John Bates في أكتوبر 2011، موجها انتقادا شديدا إلى وكالة الأمن القومي بسبب الاعتراضات التي تستند إلى المادة 702 بوجه عام. إن حقيقة أن الاتصالات المحلية كانت تعلق في تلك «المجموعات التمهيدية (الأولية)» - كما كانت تسمى - كانت متعمدة ولم تكن من قبيل المصادفة، كتب بيتس في قراره، إنها كانت جزءا متأصلا من البرنامج، وهي جزء أصيل من تكنولوجيا تبديل الحزم (packet-switching technology). من ثم، وعلى نحو يستحيل تفاديه، فإن وكالة الأمن القومي كانت كل عام تجمع «عشرات الآلاف من الاتصالات المحلية الكاملة»[23]، وهذا في حد ذاته يعد انتهاكا صارخا للتعديل الرابع لدستور الولايات المتحدة.

خلص بيتس إلى أن «الحكومة أخفقت في إثبات أنها حققت توازنا معقولا بين احتياجاتها من المعلومات الاستخباراتية الأجنبية والتزامها نحو حماية المعلومات المتعلقة بأشخاص تابعين للولايات المتحدة». نتيجة لذلك أمر بيتس بإغلاق برنامج

المادة 702 بكامله إلى أن تستحدث وكالة الأمن القومي وسيلة إصلاح من شأنها تحقيق هذا التوازن، وأمر الوكالة بحذف جميع ملفات البيانات التمهيدية (الأولية) التي كانت قد جمعتها حتى تاريخه.

أقر مقدمو الإحاطة بأن هذه كانت مشكلة قانونية مهمة، لكنهم أكدوا أنها كانت قد وصلت إلى انتباه المحكمة بواسطة وكالة الأمن القومي؛ لم يكن هناك تغطية على تجاوزات أو مخالفات. بعد قرار بيتس غيرت وكالة الأمن القومي بنية نظام التجميع بطريقة كانت ستعمل على خفض الانتهاكات المستقبلية إلى أدنى حد ممكن. شُغِّل النظام الجديد قبل شهر من تشكيل مجموعة المراجعة، وأعلن القاضي بيتس ذاته عن اقتناعه وارتياحه إلى أن هذا الأسلوب حل المشكلة.

بصورة عامة كان اليوم الأول لعمل مجموعة المراجعة مثمرا. كان الحاضرون حول الطاولة من مسؤولي وكالة الأمن القومي قد أجابوا عن كل سؤال، وتناولوا معالجة كل اعتراض أو طعن بما بدا أنه صراحة تامة، بل حتى اهتمام بمناقشة القضايا. هم نادرا ما كانوا قد ناقشوا هذه الأمور مع أناس خارجيين غرباء؛ حتى ذلك الحين، لم يكن مصرحا لأي طرف خارجي أن يناقشها، وبدا أنهم ينتهزون هذه الفرصة. كان جيوفري ستون على وجه الخصوص معجبا؛ بدا هذا المساق كأنه حلقة دراسية جامعية أكثر من كونه إحاطة داخل أكثر دوائر الاستخبارات الأمريكية تقوقعا وانعزالا.

بدا جليا أيضا أن وثائق سنودن كانت مبالغا فيها إلى حد ما، هذا إذا كان المسؤولون يقولون الحقيقة (افتراض كانت مجموعة المراجعة ستتحقق منه قريبا). بمرور اليوم فإن فرضية ستون أن وكالة الأمن القومي كانت قد تحولت إلى وكالة مارقة بدت غير صحيحة، إذ إن البرامج التي كشف عنها سنودن (مجددا، بافتراض أن الإحاطات كانت دقيقة) كانت قد صُرِّح بها، وقد وُوفق عليها، ورُصدت من كثب. معظم الضوابط والتوازنات التي كان ستون قد فكر بشأن اقتراحها تبين أنها كانت موجودة بالفعل.

لكن بالنسبة إلى بعض أعضاء اللجنة[24]، وبالقطع بالنسبة إلى ستون، وسواير، وكلارك، لم تكن الإحاطات قد بددت جانبا كبيرا من المخاوف التي كانت تسريبات سنودن قد أثارتها. هؤلاء المسؤولون من وكالة الأمن القومي، الذين قدموا الإحاطة

لهم طوال اليوم، بدوا مثل أناس موقَّرين محترمين؛ فالإجراءات الوقائية في موضع التنفيذ، ومعايير الانضباط كانت باهرة؛ بوضوح، لم يكن هذا مثل وكالة الأمن القومي في الستينيات من القرن العشرين، ولا مثل دائرة استخبارات في أي دولة أخرى. لكن، ماذا لو تعرضت الولايات المتحدة للمزيد من الهجمات الإرهابية؟ أو ماذا لو جاء إلى السلطة رئيس من نوع مختلف، أو مدير لوكالة الأمن القومي مارق بحق؟ تلك القيود كانت قد وُضعت داخليا، وكان يمكن إزالتها داخليا أيضا. من الجلي أن البراعة التقنية للوكالة كانت هائلة وصاعقة، إذ إن محلليها كان بإمكانهم النفاذ إلى كل شبكة، أو مخدم حاسوبي، أو اتصال هاتفي، أو بريد إلكتروني كانوا يريدونه. ربما منعهم القانون من الاطلاع على محتويات تلك التبادلات أو الاستماع إليها، ولكن إذا غُيِّر القانون أو تُجوهِل، فلن تكون هناك عوائق مادية. إذا أُعيد تصميم البرمجية لتعقب المنشقين السياسيين بدلا من الإرهابيين فلن تكون هناك مشكلة في تجميع قواعد بيانات ضخمة بشأن هذه الأنواع من الأهداف.

باختصار كان هناك رجحان هائل للتعسف ولتجاوزات إساءة الاستخدام. ستون، الذي كتب كتابا عن قمع المعارضة في التاريخ الأمريكي، كان يرتعد من فكرة ما الذي كان ربما سيفعله الرئيس ريتشارد نيكسون Richard Nixon، أو مدير مكتب التحقيقات الفدرالي جيه. إدجار هوفر J. Edgar Hoover إذا كانت لديهما هذه التكنولوجيا في متناول أيديهما. ومن الذي كان سيستطيع القول - لاسيما في عصر الإرهاب - إن الأمريكيين لن يروا أمثال نيكسون أو هوفر ثانية في المستويات العليا للسلطة؟

نمّى ستون تحولا غير متوقع إلى هذا الرأي لدى مايك موريل، رجل الاستخبارات المتقاعد حديثا. كان الاثنان يتشاركان أحد المكاتب في موقع «سكيف» في شارع كيه، وكان ستون، المحاضر ذو الشخصية الجذابة، يحدد المسارات المتعددة للتعسف المحتمل، بالإضافة إلى ما حدث من تعسف فعلي في الآونة الأخيرة. تاريخ زعم موريل أنه لا يعرف عنه سوى القليل، على الرغم من العقود الثلاثة التي أمضاها في وكالة الاستخبارات المركزية (أثناء جلسات استماع لجنة «تشيرش»، كان موريل في المدرسة الثانوية، غافلا عن الشؤون العالمية؛ وكان وضعه في لانغلي، حيث التحق للعمل بعد تخرجه في الجامعة مباشرة، هو رجلَ الشركة الذي يعمل بجد وعلى نحو مستمر).

على مدار الأشهر الأربعة التالية عادت المجموعة إلى «فورت ميد» بضع مرات، وكذلك زارت وفود من «فورت ميد» المجموعة في مكتبها بضع مرات. كلما ازدادت الملفات التي كانت تفحصها المجموعة وموظفوها، ازداد شعورهم بتأكيد انطباعاتهم من الإحاطة الأولى.

كان موريل هو الذي يتمعن في ملفات قضايا وكالة الأمن القومي، بما في ذلك البيانات الخام غير المعالجة التي تخص جميع المؤامرات الإرهابية الأربع والخمسين التي ادعى كل من ألكسندر وإنجليس أنها عُرقِلت بسبب برنامج «بريزم» (PRISM) بموجب المادة 702 من قانون مراقبة الاستخبارات الأجنبية، بالإضافة إلى بضع مؤامرات كانوا الآن، في مرحلة متأخرة، يدّعون أنها أُحبِطت بسبب جمع البيانات الواصفة الهاتفية، المخولة بموجب المادة 215 من قانون مكافحة الإرهاب. استنتج موريل وموظفو اللجنة[25] الذين راجعوا أيضا الملفات، أن اعتراضات برنامج «بريزم» أدت دورا في إيقاف ثلاث وخمسين مؤامرة من هذه المؤامرات الأربع والخمسين، وهذا تَثَبُّت رائع من صحة برنامج مكافحة الإرهاب المركزي بوكالة الأمن القومي وجدير بالملاحظة. مع ذلك لم يجدوا في أي من هذه الملفات الثلاثة والخمسين[26] دليلا على أن البيانات الواصفة أدت دورا جوهريا، كما أنهم لم يقتنعوا بالحالات الجديدة القليلة التي كان ألكسندر قد أرسلها إلى المجموعة؛ نعم، ظهر في تلك الحالات رقم هاتف أحد الإرهابيين في البيانات الواصفة، لكنه ظهر أيضا في عدة اعتراضات أخرى. إذا لم تكن هناك المادة 215 قط، ولم تُجمع البيانات الواصفة بكميات كبيرة وعلى نحو مجمع، فإن وكالة الأمن القومي أو مكتب التحقيقات الفدرالي كانا مع ذلك سيكتشفان تلك المؤامرات.

جاء هذا الاستنتاج مفاجئا. كان موريل يميل إلى افتراض أن البرامج الاستخباراتية التي تتلقى الثناء والإطراء بدرجة عالية من شأنها أن تسفر عن نتائج. على العكس من ذلك أدت النتائج التي توصل إليها إلى أن أوصى كلارك، وستون، وسواير بإنهاء برنامج البيانات الواصفة على الفور. لم يكن موريل على استعداد إلى الذهاب إلى هذا الحد؛ وكذلك كان صنشتاين. كلاهما كان يتبنى الحجة القائلة بأنه حتى لو أنها لم تكن قد أوقفت أي مؤامرات حتى الآن، فهي ربما تفعل ذلك في المستقبل. ذهب موريل إلى ما هو أبعد من ذلك، دافعا بحجة أن غياب النتائج كان يشير إلى أنه كان

من الضروري تكثيف البرنامج. ظن أعضاء المجموعة بعض الوقت أنه سيتعين عليهم إصدار حكم منفصل بشأن هذه القضية.

بعد ذلك، أثناء أحد الاجتماعات في «فورت ميد»، قال الجنرال ألكسندر للمجموعة إنه كان يمكنه التعايش مع ترتيب يسمح لشركات الاتصالات بالاحتفاظ بالبيانات الواصفة، ويمكن لوكالة الأمن القومي الحصول على إمكانية الوصول إلى أجزاء محددة منها فقط عن طريق إذن محكمة قانون مراقبة الاستخبارات الأجنبية. ربما يستغرق الأمر وقتا أطول قليلا للحصول على البيانات، لكنه ليس كثيرا، ربما بضع ساعات. وكان يمكن أن تنص القاعدة الجديدة التي اقترحها ألكسندر، على استثناءات تسمح بإمكانية الوصول إليها بإذن من المحكمة بأثر رجعي في حالة الطوارئ.

أيضا كشف ألكسندر[27] أنه كان لدى وكالة الأمن القومي برنامج للبيانات الواصفة للإنترنت، لكنه ثبت أنه مكلف جدا، ولم يثمر أي نتائج؛ لذا أنهاه في العام 2011.

بالنسبة إلى أعضاء مجموعة المراجعة من المتشككين فإن هذا الخبر عمق شكوكهم بشأن المادة 215 وفائدة البيانات الواصفة بوجه عام. كانت لدى وكالة الأمن القومي موازنة تقدر بمليارات الدولارات؛ فلو كانت البيانات الواصفة للإنترنت قد أسفرت عن أي شيء واعد، لكان ألكسندر قد أنفق المزيد من المال لتوسيع نطاق وصولها وانتشارها. حقيقة أنه لم يفعل ذلك، وحقيقة أنه أنهى البرنامج بدلا من مضاعفة الاستثمار فيه، ألقتا بالشكوك حول قيمة المفهوم ذاته.

حتى موريل وصنشتاين بدا أنهما يُلطفان من تشدد مواقفهما، فإذا كان ألكسندر راضيا بشأن تخزين البيانات الواصفة خارج وكالة الأمن القومي، فربما يكون ذلك بمنزلة حل وسط كان يمكن أن تقف المجموعة بأسرها خلفه وتدعمه. احتضن موريل الفكرة بحماس خاص، إذ إن البيانات الواصفة كانت ستظل موجودة، لكن إزالتها من مقر وكالة الأمن القومي كانت ستمنع مديرا مستقبليا مارقا من فحص البيانات كما يحلو له، وكانت ستقلل إلى أدنى حد من احتمالية التعسف وإساءة الاستخدام التي كان ستون قد أقنعه بأنها كانت قضية خطيرة.

كان الخلاف القصير المقتضب بشأن البيانات الواصفة، إما إنهاء البرنامج وإما توسيعه، قد أثار واحدة من بضع نوبات من الضغينة داخل المجموعة. لقد كانت

هذه الحقيقة مصدرا آخر للدهشة، إذ إنه نظرا إلى خلفياتهم ومعتقداتهم المتباينة، كان من المتوقع أن يمسك الأعضاء بعضهم برقاب بعض ويتبادلوا الهجوم باستمرار. مع ذلك كانت الأجواء متناغمة وفي وئام منذ البداية.

ترسخت هذا المودة في اليوم الثاني من عملهم، حينما ذهب الخمسة إلى بناية جي إدغار هوفر J. Edgar Hoover، مقر مكتب التحقيقات الفدرالي في وسط واشنطن. كان موظفو المجموعة قد طلبوا إحاطات تفصيلية بشأن علاقة المكتب بوكالة الأمن القومي، وعن نسخته من برنامج جمع البيانات الواصفة، المعروف باسم «خطابات الأمن القومي» (National Security Letters)، والتي بموجب المادة 505 من قانون مكافحة الإرهاب، كانت تسمح بإمكانية الوصول إلى سجلات الهاتف الخاصة بالأمريكيين وغيرها من المعاملات التي كان يُرتأى أنها «ذات صلة» بتحقيقات في الإرهاب، أو في أنشطة استخباراتية خفية. خلافا لبرنامج البيانات الواصفة الخاص بوكالة الأمن القومي لم يكن لدى برنامج مكتب التحقيقات الفدرالي أي قيود على الإطلاق، فالخطابات لا تتطلب إذنا قضائيا من المحكمة، كان بإمكان أي ضابط ميداني استصدار خطاب بتصريح من المدير، ويحظر على متسلم الخطاب أن يكشف مطلقا عن أنه قد تسلمه. (حتى تنقيح العام 2006 لم يكن يمكنهم حتى إخطار محاميهم). لم يكن الأمر يقتصر على مجرد احتمال التعسف وإساءة الاستخدام، ولكن بدا أنه من المرجح جدا حدوث حالات فعلية من التعسف وإساءة الاستخدام.

حينما وصل الأعضاء الخمسة إلى مقر المكتب لم يستقبلهم المدير، ولا نائبه، ولكن استقبلهم المسؤول الثالث، الذي غادر بعد مرافقتهم إلى قاعة المؤتمرات، حيث كان يجلس عشرون من مسؤولي مكتب التحقيقات الفدرالي حول طاولة، جاهزين لتقديم عروض رتيبة معلبة، واصفين مهامهم ووظائفهم الواحد تلو الآخر، طوال الساعة التي خصصت للمجموعة.

بعد عشر دقائق من هذا العرض المستفيض سأل كلارك بشأن الإحاطات التي كانت المجموعة قد طلبتها، كان يريد أن يعرف على وجه التحديد عدد خطابات الأمن القومي التي كان مكتب التحقيقات الفدرالي يصدرها كل عام، وكيف كان المكتب يقيس فعاليتها. أجاب أحد المسؤولين بأن المكاتب الإقليمية هي وحدها

التي كانت لديها تلك الأرقام، ولم يكن أحد قد جمعها على الصعيد القومي، أو وضع أي مقياس للفعالية.

استؤنفت الإحاطات المعلبة الرتيبة، لكن بعد بضع دقائق أخرى، وقف كلارك مشدوها وصاح: «هذا هراء[28]. نحن خارجون من هنا». خرج من الغرفة، وتبعه الأربعة الآخرون في خجل، في حين جلس مسؤولو مكتب التحقيقات الفدرالي في حالة من الصدمة والذهول. في البداية كان أيضا زملاء كلارك يشعرون بالخزي بعض الشيء، وكانوا قد سمعوا بشأن تصرفاته وألاعيبه الغريبة، وتساءلوا عما إذا كان هذا سيكون إجراء معتادا.

لكن في اليوم التالي كان جليا أن كلارك عرف تماما ما الذي كان يفعله، إذ إنه سرعان ما انتشر خبر «الإحاطة الهزلية». ومن تلك النقطة فصاعدا لم تجرؤ أي دائرة فدرالية على إهانة المجموعة بعروض تقديمية تعليمية متعالية؛ بضع دوائر فقط هي التي ثبت أنها ذات فائدة كبيرة، لكن جميعهم حاولوا على الأقل أن يكونوا موضوعيين، وحتى مكتب التحقيقات الفدرالي عاود الاتصال بهم للحصول على فرصة ثانية.

شجع تصرف كلارك زملاءه على الضغط بحزم أكثر من أجل الحصول على إجابات عن أسئلتهم. عززت طبيعة عملهم هذا التضافر. هم كانوا أول مجموعة من أناس خارجيين تُدعى للتحقيق في هذا الموضوع بدعم من الرئيس، وهم استمدوا روح الجماعة من هذا التميز. إضافة إلى ذلك فقد وجدوا أنفسهم يتفقون على كل شيء تقريبا، لأن معظم الحقائق كانت تبدو جلية جدا. حتى بيتر سواير، الذي كان قلقا من تأجيج توترات مع كلارك مضى عليها خمسة عشر عاما، وجد نفسه أنه كلما كان على وفاق مع غريمه السابق ويكتسب ثقة بتقديراته وأحكامه كانوا أكثر توافقا مع أحكامه.

بينما كانت الأجواء تتلطف من الألفة إلى البهجة بدأوا يطلقون على أنفسهم اسم «الرفاق الخمسة»، نسبة إلى اسم مطعم هامبرغر محلي، وإشارة إلى الكتاب الكبير الذي كانوا سيكتبونه قريبا على أنه «تقرير الرفاق الخمسة» (The Five Guys Report).

قويت لديهم روح الجماعة مع إدراكهم أنهم كانوا إلى حد كبير هم الراصدين الجادين الوحيدين في المدينة. اجتمعوا في «كابيتول هيل» مع اللجان المختارة المعنية

بالاستخبارات، وخلصوا إلى أن أعضاءها لم يكن لديهم الوقت ولا الموارد للمراقبة بعمق؛ وتحدثوا مع بضعة قضاة سابقين من محكمة قانون مراقبة الاستخبارات الأجنبية، ووجدوا أنهم توافقيون جدا بطبيعتهم.

ثمة شيء جيد، أنهم خلصوا إلى استنتاج مفاده أن جهاز الأمن القومي كان لديه جيش داخلي من المحامين لضمان التوافق مع القواعد والالتزام بها، لأنه إذا لم يفعل ذلك، فإن أي شخص خارجي كان سيعدم وسيلة لمعرفة ما إذا كان - أو لم يكن - الجهاز وكرا من الفوضى والخروج على القانون. اتفق الرفاق الخمسة على أن مهمتهم، قبل كل شيء آخر، كانت هي التوصل إلى سبل لتعزيز الضوابط الخارجية.

وزعوا مهام الكتابة، كل منهم يعد مسودة قسم أو قسمين، ويدرج أفكارا حول كيفية إصلاح المشكلات التي شُخِّصت. قصّوا، ولصقوا، ونقحوا، وحرروا الأقسام إلى أن توصلوا إلى تقرير مكون من 303 صفحات، مع 46 توصية بالإصلاح.

نبعت إحدى التوصيات الرئيسية من محادثة المجموعة مع الجنرال ألكسندر، إذ إنه كان لزاما إزالة كل البيانات الواصفة من «فورت ميد»، والاحتفاظ بها لدى شركات الاتصالات الخاصة، أو لدى أي طرف ثالث آخر، مع عدم السماح لوكالة الأمن القومي بإمكانية الوصول إلا بإذن من محكمة قانون مراقبة الاستخبارات الأجنبية. كانت المجموعة متشددة بشأن هذه النقطة على نحو خاص. حتى مايك موريل كان قد توصل إلى اعتبار هذه التوصية على أنها محور التقرير، كان يشعر بأنه إذا رفضها الرئيس فإن العملية برمتها ستكون بلا جدوى.

كان هناك اقتراح آخر ينص على منع مكتب التحقيقات الفدرالي من إصدار خطابات الأمن القومي من دون إذن من محكمة قانون مراقبة الاستخبارات الأجنبية، وفي كل الأحوال، بعد 180 يوما يسمح لمتسلمي الخطاب بالكشف عن أنهم كانوا قد تلقوا مثل هذا الخطاب، ما لم يأذن القاضي بتمديد مدة سرية الخطاب لأسباب خاصة تتعلق بالأمن القومي. وفقا لما ورد في التقرير كان الهدف من كلتا التوصيتين هو «الحد من احتمالات[29] تعسف الحكومة، سواء الفعلية أو المفترضة».

أيضا كتبت المجموعة أنه كان ينبغي أن تتضمن محكمة قانون مراقبة الاستخبارات الأجنبية مدافعا عن المصلحة العامة، وأن مجلس الشيوخ كان ينبغي أن يعتمد مديري وكالة الأمن القومي، الذين لا ينبغي لهم تولي المنصب

الإضافي للقيادة السيبرانية للولايات المتحدة (على أساس أن الرئاسة المزدوجة للقيادة السيبرانية ولوكالة الأمن القومي كانت تمنح نفوذا أكثر مما ينبغي لشخص واحد)، وأنه كان ينبغي فصل مديرية ضمان المعلومات - وجه «فورت ميد» المتعلق بالأمن السيبراني - عن وكالة الأمن القومي وتحويلها إلى دائرة منفصلة تابعة لوزارة الدفاع.

كانت هناك توصية أخرى تتمثل في منع الحكومة من فعل أي شيء من شأنه «تخريب، أو تعطيل، أو إضعاف[30] البرمجيات التجارية المتاحة، أو جعلها على نحو عام عرضة للهجوم». على وجه التحديد، إذا اكتشف محللو وكالة الأمن القومي إحدى الثغرات الأمنية التي يمكن استغلالها بشكل فوري من دون انتظار، والتي لم يكن أحد قد اكتشفها بعد (نقاط الضعف الفورية)، كان يتعين إلزامهم بإصلاح الثغرة في الحال، باستثناء «حالات نادرة»، حينما كانت الحكومة تستطيع منح «تصريح قصير» لاستخدام تلك الثغرات «لجمع معلومات استخباراتية ذات أولوية قصوى». على الرغم من ذلك، وحتى في هذه الحالة، لم يكن في استطاعتهم القيام بذلك إلا بعد موافقة لجنة «مراجعة عليا مشتركة بين الوكالات تضم كل الوزارات المعنية».

كانت هذه هي إحدى توصيات المجموعة الأكثر انحصارا على فئة معينة، لكنها كانت توصية جوهرية أيضا. كانت الثغرات الأمنية التي يمكن استغلالها بشكل فوري من دون انتظار، والتي لم يكن أحد قد اكتشفها بعد (نقاط الضعف الفورية) هي جواهر استخبارات الإشارة (سيجينت) العصرية، والسلع الثمينة التي كانت الوكالة تدرب كبار مخبريها على الكشف عنها واستغلالها، وأحيانا كانت تدفع أموالا لقراصنة حاسوب خصوصيين لهذا الغرض. كان المقصود من الاقتراح؛ من ناحية، استرضاء المديرين التنفيذيين لشركات البرمجيات الأمريكية، والذين كانوا قلقين من أن السوق الخارجية كانت ستنضب إذا افترض الزبائن المرتقبون أن وكالة الأمن القومي حفرت أبوابا خلفية في منتجاتهم. لكنه كان يهدف أيضا إلى أن تكون شبكات الحاسوب أقل عرضة للهجوم. إنه كان إعلانا عن أن احتياجات الأمن السيبراني كان يتعين أن تعلو على احتياجات وسائل الحرب السيبرانية الهجومية.

ختاما، وخشية أن يفسر أي شخص التقرير[31] على أنه تبرير لما فعله إدوارد سنودن (الذي لم يظهر اسمه في أي مكان في النص)، فإن عشرا من التوصيات الست والأربعين تناولت سبلا للتشديد الأمني على المعلومات المصنفة داخل الأوساط الاستخباراتية على أنها سرية جدا، بما في ذلك إجراءات منع مسؤولي النظام - الوظيفة التي كان سنودن قد شغلها في منشأة وكالة الأمن القومي في «أواهو» - من الوصول إلى الوثائق التي ليس لعملهم علاقة بها.

إنها كانت مجموعة من المقترحات المتنوعة واسعة النطاق. الآن ماذا نفعل بها؟ حينما التقى الخمسة للمرة الأولى في أواخر شهر أغسطس، كانوا قد بدأوا نقاشا بشأن كيفية التعامل مع نقاط عدم الاتفاق العديدة التي كانوا يتوقعونها. هل كان ينبغي أن يحتوي التقرير على حواشٍ للآراء المخالفة، أم فصول للأغلبية وأخرى للأقلية، أم ماذا؟ هم لم يكونوا قد أتموا ذلك النقاش بعد؛ والآن، ها هم، والموعد النهائي أصبح وشيكا، في منتصف ديسمبر.

اقترح أحد موظفي اللجنة إدراج التوصيات الست والأربعين في جدول بيانات «إكسل» Excel، ووضع «نعم» أو «لا» قرين كل منها، وأن يأخذ كل عضو من الأعضاء الخمسة نسخة من الجدول، ويضع علامة تشير إلى ما إذا كان موافقا أو غير موافق على كل توصية. ثم يجدول الموظف النتائج.

بعد عد الأصوات، نظر الموظف إلى أعلى، وقال: «لن تصدقوا هذا». كان الرفاق الخمسة قد وافقوا بالإجماع على التوصيات الست والأربعين جميعها.

في 13 ديسمبر[32]، قبل الموعد النهائي بيومين، سلم أعضاء مجموعة المراجعة تقريرهم، بعنوان «الحرية والأمن في عالم متغير» Liberty and Security in a Changing World. كان في اعتقادهم أنهم استوفوا مهمتهم الرئيسية، وفقا لما جاء في تقريرهم، «لتعزيز ثقة العامة[33]، في حين يسمح أيضا للأوساط الاستخباراتية بأن تقوم بما ينبغي القيام به للاستجابة لتهديدات حقيقية»، بل إنهم أيضا تجاوزوا ذلك التكليف المحدود، بتبيانهم إصلاحات كبيرة حقيقية لنظام جمع المعلومات الاستخباراتية.

كانت عباراتهم اللغوية صريحة ومباشرة، على نحو سيثير حتما غضب جميع أطراف النقاش الذي كان قد ازدادت حدته خلال الأشهر الستة التي تلت حملة

الوثائق التي سربها سنودن. ذكر التقرير أنه: «على الرغم من أن الإفصاحات[34] والتعليقات الأخيرة قد خلقت في بعض الأوساط انطباعا مفاده أن مراقبة وكالة الأمن القومي عشوائية من دون تمييز، ومنتشرة في جميع أنحاء العالم، فإن الأمر ليس كذلك». مع ذلك، أضاف التقرير أن مجموعة المراجعة وجدت «حالات جادة ومستمرة من عدم الامتثال في إنفاذ الأوساط الاستخباراتية سلطاتها»، التي «حتى إن كان على نحو غير متعمد»، أثارت «قلقا بالغا» بشأن «قدرتها على إدارة» سلطاتها «بطريقة فعالة وقانونية».

وبعبارة أخرى (ذكرت النقطة عدة مرات، على مدار التقرير)، في حين وجدت المجموعة «أنه لا يوجد دليل على عدم المشروعية[35]، أو غيرها من التعسف في استخدام السلطة بغرض استهداف أنشطة سياسية محلية»، كان هناك، دائما «الخطر الكامن[36] من حدوث التعسف». ذكر التقرير في إحدى الفقرات التي ربما خرجت مباشرة من كتاب جيفري ستون: «نحن لا نستطيع أن نستبعد[37] الخطر، في ضوء الدروس المستفادة من تاريخنا، في وقت ما في المستقبل، سيقرر المسؤولون الحكوميون رفيعو المستوى أن قاعدة البيانات الضخمة هذه التي تحتوي على معلومات شخصية خاصة وحساسة جدا هي هناك للاقتطاف».

في 18 ديسمبر[38]، في الساعة الحادية عشرة صباحا، التقى الرئيس أوباما مجددا بالمجموعة في غرفة العمليات. كان أوباما قد قرأ الخطوط العامة العريضة للتقرير، وكان يخطط لمطالعته في أثناء عطلة عيد الميلاد في منزله لقضاء الإجازات في «هاواي».

بعد مضي شهر، في 17 يناير من العام 2014، أعلن أوباما في خطاب ألقاه في وزارة العدل، مجموعة سياسات جديدة حث عليها التقرير. تطرق النصف الأول من خطابه إلى أهمية الاستخبارات على مدار التاريخ الأمريكي، رحلة «بول ريفير» Paul Revere، محذرا من أن البريطانيين قادمون، والبالونات الاستطلاعية التي أطلقها جيش الاتحاد لقياس حجم كتائب الكونفدراليين، والدور الحيوي الذي أداه كاسرو الشفرات في هزيمة ألمانيا النازية والإمبراطورية اليابانية. قال أوباما، على غرار ذلك، اليوم: «نحن لا نستطيع منع الهجمات الإرهابية[39]، أو التهديدات السيبرانية من دون بعض من القدرة على النفاذ إلى الاتصالات الرقمية».

كانت الرسالة قد نفذت إلى كل جنبات دواوين الجهاز الإداري للأمن القومي، وكان أوباما قد استوعبها أيضا، إذ إنه في العالم السيبراني ينشأ الهجوم والدفاع من الأدوات والتقنيات ذاتها (بعد مضي عدة أشهر، في مقابلة مع إحدى المجلات المتخصصة في تكنولوجيا المعلومات تصدر على شبكة الإنترنت، شبَّه أوباما - أشهر عشاق كرة السلة - الصراع السيبراني بكرة السلة «من حيث إنه لا يوجد خط فاصل واضح[40] بين الهجوم والدفاع، الأمور تسير جيئة وذهابا طوال الوقت»)، ومن ثم، تجاهل الرئيس مقترحات مجموعة المراجعة لإبعاد وكالة الأمن القومي عن القيادة السيبرانية، أو لوضع الجانب الدفاعي لوكالة الأمن القومي في دائرة منفصلة.

مع ذلك، وافق أوباما على النقطة العامة للمجموعة بشأن «خطر التجاوز الحكومي»، و«احتمال التعسف». وهكذا، قبل أوباما كثيرا من توصياتها الأخرى. رفض أوباما الاقتراح الذي كان يقضي بطلب إذن محكمة قانون مراقبة الاستخبارات الأجنبية لخطابات الأمن القومي الخاصة بمكتب التحقيقات الفدرالي، لكنه حدد مدة بقاء الرسائل مصنفة على أنها سرية (استقر في النهاية على مهلة مدتها 180 يوما، والتمديد يستلزم إذنا قضائيا). لن يكون هناك مزيد من المراقبة «لأصدقائنا وحلفائنا المقربين»، من دون سبب مقنع (إشارة إلى مراقبة هاتف أنجيلا ميركل الجوال، على الرغم من أن صياغة أوباما سمحت بمجال واسع للاستثناءات). كان فريق الأمن القومي التابع له سيجري مراجعات سنوية لبرامج المراقبة، وتقييم الاحتياجات الأمنية مقابل السياسات تجاه الحلفاء، وحقوق الخصوصية، والحريات المدنية، والمصالح التجارية للشركات التابعة للولايات المتحدة.

بعد مضي ثلاثة أشهر، أدت هذه الفكرة الأخيرة إلى سياسة جديدة للبيت الأبيض تحظر استخدام أداة برمجية للاستغلال الفوري من دون انتظار الثغرات الأمنية التي لم يكن أحد قد اكتشفها بعد (نقاط الضعف الفورية)، ما لم تقدم وكالة الأمن القومي حجة دامغة بأن الإيجابيات تفوق السلبيات. وكان القرار النهائي في هذا الشأن لن يقرره مدير وكالة الأمن القومي، ولكن سيكون من قبل الوزراء الأعضاء في مجلس الأمن القومي، وفي النهاية، من قبل الرئيس. كان هذا

من المحتمل أن يكون أمرا مهما للغاية. أما إذا كان الأمر سيحد من الممارسة فعلا، أو إذا كان الأمر بمنزلة فحص سياسي أو ختم مطاطي، فهذا شأن آخر(*).

أخيرا، تحدث أوباما بشأن أكثر البرامج إثارة للجدل، التجميع الضخم بالجملة للبيانات الواصفة الهاتفية بموجب المادة 215 من قانون مكافحة الإرهاب. أولا، كخطوة فورية، أمر أوباما بأن تقيد وكالة الأمن القومي عملياتها للبحث في البيانات إلى قفزتين، أقل من الحد المسموح به في السابق، وهو ثلاث قفزات (على الرغم من أنه يحتمل أن يكون ملموسا وله تأثير كبير، فإن هذا كان له تأثير ضئيل، إذ إن وكالة الأمن القومي لم تلجأ قط إلى ثلاث قفزات). ثانيا، والأهم من ذلك، هو أن أوباما اعتمد اقتراح تخزين البيانات الواصفة لدى أحد كيانات القطاع الخاص، وعدم منح وكالة الأمن القومي إمكان الوصول إلا بعد استصدار إذن من محكمة قانون مراقبة الاستخبارات الأجنبية.

بدت تلك التصديقات محكوما عليها بالفشل ومصيرها الهلاك، لأن أي تغييرات في تخزين البيانات الواصفة، أو في تشكيل محكمة قانون مراقبة الاستخبارات الأجنبية، كان لزاما أن يقترع عليه الكونغرس. في ضوء الظروف العادية، فإن الكونغرس - لاسيما هذا الكونغرس الذي كان يسيطر عليه الجمهوريون - لم يكن ليحدد موعدا لإجراء مثل هذا الاقتراع، إذ لم يكن لدى قادته الرغبة في تغيير عمليات دوائر الاستخبارات، أو القيام بالكثير من أي شيء كان الرئيس أوباما يرغب في أن يفعلوه.

لكن تلك لم تكن أحوالا عادية. كان الكونغرس، تحت ضغط كبير، قد مرر القانون الأمريكي لمكافحة الإرهاب في أعقاب هجمات 11 سبتمبر، إذ إن مشروع القانون جاء إلى أعضاء الاجتماع ساخنا من المطابع، وتقريبا لم يكن لدى أحد الوقت

(*) الأسئلة التي تُطرَح[41] عند النظر فيما إذا كان ينبغي استغلال الثغرات الأمنية التي يمكن استغلالها على نحو فوري من دون انتظار، والتي لم يكن أحد قد اكتشفها بعد («نقاط الضعف الفورية»)، كانت هي: مدى استخدام النظام الذي يحوي الثغرة الأمنية في البنية الأساسية الحرجة؛ بعبارة أخرى، إذا تركت الثغرة الأمنية من دون إصلاحها، هل تشكل على مجتمعنا أخطارا لها تأثير كبير ملموس؟ إذا عرف أحد الخصوم أو المجموعات الإجرامية بشأن الثغرة الأمنية، فما مدى الضرر الذي كان يستطيع أن يلحقه؟ ما احتمالية أننا كنا سنعرف ما إذا أقدم أحد آخر على استغلالها؟ ما مدى احتياجنا إلى المعلومات الاستخباراتية التي نعتقد أننا نستطيع الحصول عليها من استغلالها؟ هل هناك طرق أخرى للحصول على هذه المعلومات الاستخباراتية؟ هل كان يمكننا استغلال الثغرة الأمنية فترة زمنية قصيرة قبل الكشف عنها وتصحيحها؟

لقراءته. في مقابل التسرع في تمريره، وإزاء معارضة شديدة من بوش والبيت الأبيض، أصر الديموقراطيون الرئيسيون من المشرعين أعضاء المجلس على أن يكتب شرط النسخ التلقائي - تاريخ انقضاء الصلاحية - في أجزاء معينة من القانون (بما في ذلك المادة 215، التي كانت تسمح لوكالة الأمن القومي بجمع البيانات الواصفة وتخزينها)، حتى يتمكن الكونغرس من تمديد أحكامه، أو أن يدعها تنصرم وتنتهي حينما يتطلب الأمر مزيدا من المداولات.

في العام 2011، حينما كان سريان مفعول تلك الأحكام قد أوشك على الانتهاء أخيرا، اقترع الكونغرس على تمديدها حتى يونيو من العام 2015. في أثناء تلك السنوات الأربع، حدثت ثلاثة أمور: أولا، وعلى نحو محوري بالغ الأهمية، جاءت مكاشفات إدوارد سنودن بشأن مدى اتساع المراقبة المحلية التي تضطلع بها وكالة الأمن القومي. ثانيا، خلص تقرير الرفاق الخمسة إلى أن هذه البيانات الواصفة لم تكن قد أدت إلى اعتقال أي إرهابي، وأوصى التقرير بإجراء إصلاحات كثيرة للحد من احتمال التعسف في استخدام السلطة.

ثالثا، في 7 مايو، قبل تاريخ انتهاء الصلاحية التالي بأسابيع فقط، أصدرت الدائرة الثانية لمحكمة الاستئناف بالولايات المتحدة حكما مفاده أن المادة 215 من قانون مكافحة الإرهاب هي في الواقع لم تخول أي شيء فضفاض، مثل برنامج وكالة الأمن القومي للجمع الضخم بالجملة للبيانات الواصفة؛ وأن البرنامج في الواقع غير قانوني. كانت المادة 215 تسمح للحكومة باعتراض وتخزين البيانات التي كانت لها «صلة» بـ «تقصٍّ» في مؤامرة أو مجموعة إرهابية. بررت وكالة الأمن القومي بأنه في تتبع روابط وعلاقات مؤامرة إرهابية، كان من المستحيل معرفة ما هو ذو صلة - من هم الأطراف الفاعلون - في وقت مبكر قبل الأوان، لذلك كان من الأفضل إنشاء أرشيف للمكالمات التي كان يمكن أن يُبْحَث فيها بأثر رجعي. بهذا المنطق، كان من الضروري جمع كل شيء؛ لأن أي شيء ربما يثبت أنه ذو صلة؛ للعثور على إبرة في كومة قش، فأنت في حاجة إلى إمكان الوصول إلى «كومة القش بكاملها». كانت محكمة قانون مراقبة الاستخبارات الأجنبية قد قبلت منذ وقت طويل منطق وكالة الأمن القومي، ولكن الآن رفضت محكمة الدائرة الثانية هذا الأمر على أنه «غير مسبوق وغير مبرر»[42]. في جلسة المحكمة التي أسفرت عن الحكم، شبهت وزارة

العدل (التي كانت تدافع عن موقف وكالة الأمن القومي) برنامج جمع البيانات الواصفة بسلطات الأمر بالاستدعاء الواسعة المخولة لهيئة المحلفين الكبرى. غير أن المحكمة استهجنت هذا القياس، وذكرت أن هيئات المحلفين الكبرى «مقيدة بحقائق» تخص تحريا بعينه، و«بقيود زمنية محدودة»، في حين أن برنامج وكالة الأمن القومي للبيانات الواصفة كان يتطلب «أن تسلم شركات الهاتف السجلات «يوميا على نحو مستمر»، من دون نقطة نهاية منظورة، ولا يتطلب الأمر أي صلة بأي مجموعة حقائق محددة، ومن دون قيود على الموضوعات أو الأفراد الذين كان يجري تغطيتهم».

امتنع القضاة عن الحكم على دستورية البرنامج، وسمحوا بأنه يمكن للكونغرس أن يجيز برنامج البيانات الواصفة، إذا اختار أن يفعل ذلك علنا. وهكذا كان الأمر متروكا للكونغرس، ولم يكن في مقدور أعضائه التهرب من اللحظة الحاسمة. بسبب شرط النسخ التلقائي، كان لزاما على مجلس النواب ومجلس الشيوخ الاقتراع على المادة 215، بطريقة أو بأخرى؛ إذا لم يفعلوا ذلك، فإن برنامج البيانات الواصفة كان سينتهي تلقائيا.

في هذا المناخ المشوه، لم يستطع الزعماء الجمهوريون حشد دعم الأغلبية للإبقاء على الوضع الراهن. أعد المعتدلون في الكونغرس مسودة مشروع قانون يسمى «قانون حرية الولايات المتحدة الأمريكية» USA Freedom Act الذي كان سيبقي البيانات الواصفة مخزنة لدى شركات الاتصالات، ولا يسمح لوكالة الأمن القومي بالوصول إلا إلى أجزاء محددة منها، وفقط بعد الحصول على إذن من محكمة قانون مراقبة الاستخبارات الأجنبية للقيام بذلك. كان القانون الجديد سيلزم أيضا محكمة قانون مراقبة الاستخبارات الأجنبية بتعيين مناصر للحريات المدنية ليترافع أحيانا ضد طلبات وكالة الأمن القومي. وكان الأمر سيتطلب إجراء مراجعات دورية لرفع السرية عن أجزاء، على الأقل، من قرارات محكمة قانون مراقبة الاستخبارات الأجنبية. أقر مجلس النواب مشروع القانون الإصلاحي بأغلبية كبيرة؛ أما مجلس الشيوخ، بعد ممانعة كبيرة من قيادات الجمهوريين، فلم يكن لديه خيار سوى تمريره كذلك.

على الرغم من كل الصعاب، بسبب حيطة حكيمة متبصرة بعواقب قانون تم تمريره في العام 2001 وسط هلع حالة طوارئ قومية، أقر الكونغرس الإصلاحات

الرئيسية لممارسات وكالة الأمن القومي، على النحو الذي أوصت به لجنة الرئيس أوباما، والرئيس أوباما ذاته.

لم تكن التدابير ستغير كثيرا بشأن الجاسوسية السيبرانية، أو الحرب السيبرانية، أو اليد الطولى لوكالة الأمن القومي، فضلا على الجهات المناظرة الأجنبية. على الرغم من العواصف السياسية التي أثارها التجميع الضخم بالجملة للبيانات الواصفة المحلية، فإنه كان يشكل جزءا ضئيلا من أنشطة الوكالة. لكن الإصلاحات كانت ستعيق دربا محتملا مغريا للتعسف وإساءة استخدام السلطة، ووضعت مستوى إضافيا من السيطرة الرقابية - وإن كان طبقة رقيقة - على نفوذ الوكالة، ونزعة تكنولوجياتها نحو التسلل إلى الحياة اليومية والتطفل عليها.

في 31 مارس، بعد مضي شهرين ونصف الشهر من خطاب أوباما في وزارة العدل الذي دعا فيه إلى تلك الإصلاحات، ألقى جيفري ستون خطابا في «فورت ميد». كان موظفو وكالة الأمن القومي قد طلبوا منه أن يسرد عليهم عمله في مجموعة المراجعة، ويجتلي الأفكار والدروس التي خرج بها.

بدأ ستون بالإشارة إلى أنه، باعتباره ليبراليا علمانيا مؤمنا بالحريات المدنية، كان قد اقترب من وكالة الأمن القومي بتشكك كبير، ولكنه سرعان ما تأثر بما لديها من «قدر كبير من النزاهة»، و«التزام عميق بسيادة القانون». لا شك في أن الوكالة ارتكبت أخطاء، لكنها كانت أخطاء فقط، وليست أفعالا غير مشروعة متعمدة. إنها لم تكن وكالة مارقة، إنها كانت تقوم بما كان يريده رؤساؤها السياسيون، وما كانت تسمح به المحاكم؛ وبينما كانت الإصلاحات ضرورية، كانت أنشطتها بوجه عام قانونية.

أغدق خطابه الثناء والمديح على الوكالة وموظفيها فترة أطول قليلا، لكنه بعد ذلك أخذ منحى حادا. أكد ستون: «لكي أكون واضحا[43]، أنا لا أقول إن المواطنين ينبغي لهم أن يثقوا بوكالة الأمن القومي». كان لزاما على الوكالة أن تلتزم بـ «المراجعة الدائمة والدقيقة». كان عملها «مهما لسلامة البلاد»؛ لكنه كان بطبيعته ينطوي على «أخطار جسيمة» على القيم الأمريكية.

أوجز ستون: «ما أدهشني، أنني وجدت أن وكالة الأمن القومي تستحق احترام وتقدير الشعب الأمريكي، لكن أبدا لم يكن لزاما أن نثق بها».

15

«نحن شاردون في منطقة معتمة»

في أولى ساعات الصباح الباكر[1] من يوم الاثنين 10 فبراير 2014، بعد أربعة أسابيع من خطاب الرئيس أوباما في وزارة العدل، بشأن إصلاح وكالة الأمن القومي، شن قراصنة الحاسوب هجوما سيبرانيا ضخما واسع النطاق ضد مؤسسة «لاس فيغاس ساندز» Las Vegas Sands Corporation، المالك لفندقي القمار «فينيتيان» Venetian و«بالازو» Palazzo في شارع فيغاس ستريب Vegas Strip، ومنتجع «ذي ساندز» (الرمال) the Sands المماثل، في مدينة بيت لحم Bethlehem، بولاية بنسلفانيا Pennsylvania.

دمر الهجوم محركات الأقراص الصلبة في آلاف المخدمات، والحواسيب الشخصية،

«دمر الهجوم محركات الأقراص الصلبة في آلاف المخدمات، والحواسيب الشخصية، والحواسيب المحمولة، بعد سرقة بيانات بطاقات الائتمان الخاصة بآلاف العملاء»

والحواسيب المحمولة، بعد سرقة بيانات بطاقات الائتمان الخاصة بآلاف العملاء، فضلا على أسماء موظفي الشركة وأرقام الضمان الاجتماعي الخاصة بهم.

عزا متخصصو السيبرانية الهجوم إلى الجمهورية الإسلامية الإيرانية.

في شهر أكتوبر السابق (2013)، كان شيلدون أديلسون Sheldon Adelson، الملياردير اليميني المؤيد بشدة لإسرائيل، والذي كان يمتلك 52 في المائة من أسهم مؤسسة «لاس فيغاس ساندز»، قد تحدث في إحدى حلقات النقاش في «جامعة يشيفا» Yeshiva University في نيويورك؛ وعند نقطة ما، سُئل أديلسون سؤالا بشأن المفاوضات النووية التي تجريها إدارة أوباما مع إيران في الوقت الحالي.

أجاب: «ما كنت سأقوله هو، أنصت. أترى تلك الصحراء هناك؟ أنا أريد أن أريك شيئا». بعد ذلك، قال أديلسون، إنه كان سيسقط قنبلة نووية على الموقع؛ واستطرد: «لن يؤذي الانفجار نفسا، ربما بعض الأفاعي الجرسية أو العقارب أو أي شيء». لكنه يرسي إنذارا، قال إنه كان سيقول لنظام الملالي: «هل تريد أن تباد؟ هيا، تقدم واتخذ موقفا متشددا» في تلك المحادثات.

انتشر استبداد أديلسون في الرأي سريعا على يوتيوب كالنار في الهشيم. بعد مضي أسبوعين، كان آية الله علي خامنئي، المرشد الأعلى في إيران، يستشيط غضبا من أن أمريكا «كان ينبغي أن تصفع أولئك الأشخاص الثرثارين» و«تسحق أفواههم».

بعد فترة وجيزة، بدأ قراصنة الحاسوب في العمل على الشركة التي يمتلكها أديلسون. في 8 يناير، حاولوا اقتحام المخدم الحاسوبي في منتجع «ذي ساندز» (الرمال) في مدينة بيت لحم بولاية بنسلفانيا، مستكشفين محيطه بحثا عن مواطن ضعف. في الحادي والعشرين، ومجددا في السادس والعشرين، نَشَّطوا برمجية لكسر كلمة المرور، محاولين تجربة ملايين من توليفات الحروف والأرقام، على نحو آني تقريبا، لاختراق الشبكة الافتراضية الخاصة Virtual Private Network للشركة، والتي كان الموظفون يستخدمونها من منازلهم أو على الطريق.

أخيرا، في 1 فبراير، عثروا على موطن ضعف في المخدم الحاسوبي الخاص بإحدى شركات مدينة بيت لحم التي كانت تختبر صفحات جديدة لموقع الويب الخاص بنادي القمار. باستخدام أداة أطلق عليها اسم «ميميكاتز» Mimikatz التي كانت تستخلص كل سجلات المخدم logs الحديثة، عثر المخترقون على اسم المستخدم

وكلمة المرور الخاصة بمهندس النظم في شركة «ساندز»، الذي كان قد جاء من فوره إلى «بيت لحم» في رحلة عمل، باستخدام بيانات اعتماده credentials، تجول قراصنة الحاسوب في المخدمات الموجودة في فيغاس، وفحصوا مساراتها، وأدخلوا برمجية خبيثة تتكون من 150 سطرا فقط من التعليمات البرمجية (الكود)، التي محت البيانات المخزنة على كل حاسوب ومخدم، ثم ملأت الفراغات بدفقة عشوائية من الأصفار والآحاد، حتى تكون عملية استعادة البيانات مهمة شبه مستحيلة.

ثم بدأوا في تنزيل بيانات حساسة جدا، كلمات مرور خاصة بمسؤولي تكنولوجيا المعلومات، ومفاتيح فك التشفير، والتي كان يمكن أن تنقلهم إلى الحاسوب المركزي، وربما الأكثر ضررا، كان يمكن أن تنقلهم إلى ملفات كبار العملاء - «الحيتان» - كما كان أصحاب نوادي القمار يطلقون عليهم. في الوقت المناسب، أغلق المسؤولون في «ساندز» خط ربط الشركة بالإنترنت.

مع ذلك، في اليوم التالي، اكتشف المخترقون طريقا آخر للعودة؛ فشوهوا موقع الويب الخاص بالشركة، ووضعوا عليه رسالة «التشجيع على استخدام أسلحة الدمار الشامل هو جريمة تحت أي ظرف من الظروف». ثم أوقفوا تشغيل بضع مئات من الحواسيب الأخرى التي لم يكن قد جرى تعطيلها في المرة الأولى.

بعد أن هدأت العاصفة، قدر فريق الأمن السيبراني في نادي القمار أن الإيرانيين دمروا عشرين ألف حاسوب، وهو ما كان إحلالها سيكلف ما لا يقل عن 40 مليون دولار.

كان هجوما سيبرانيا نمطيا أن يحدث في العقد الثاني من القرن الحادي والعشرين، وإن كان متطورا إلى حد ما. ومع ذلك، كان هناك أمر واحد غريب بشأن هؤلاء القراصنة، إذ إن أي شخص يقتحم مخدمات نادي القمار بفندق في لاس فيغاس كان يمكنه أن يجني منه أموالا طائلة، لكن هؤلاء القراصنة لم يأخذوا سنتا واحدا. كان هدفهم الوحيد هو معاقبة شيلدون أديلسون على تصريحاته الفجة غير المهذبة بشأن تدمير إيران بالقنبلة النووية، وقد شنوا هجوما سيبرانيا ليس لسرقة أموال أو أسرار الدولة، بل للتأثير في الخطاب السياسي لرجل ذي نفوذ.

إنه كان بعدا جديدا، وحقبة جديدة، لوسائل الحرب السيبرانية.

سمة أخرى جديرة بالملاحظة، لاحظها المسؤولون التنفيذيون في «ساندز» بعد الواقعة، وهي أن الإيرانيين بعد اضطلاعهم بمثل تلك الاستعدادات المكثفة، كان

يمكنهم إطلاق العنان لمثل هذا الهجوم المدمر من دون إثارة الانتباه، لأن هيئة الأمن السيبراني في الشركة كانت تتألف من خمسة أشخاص فقط.

مؤسسة «لاس فيغاس ساندز»، أحد أكبر مجمعات المنتجعات في العالم، يعمل بها 40 ألف موظف، ولديها أصول تتجاوز 20 مليار دولار، لم تكن مجهزة للتعامل مع الحقبة القديمة للحرب السيبرانية، فضلا على التعامل مع الحقبة الجديدة.

في البداية، لم يرغب المسؤولون التنفيذيون في إخافة العملاء، فحاولوا التغطية على مدى الضرر الذي لحق بهم من جراء الاختراق، حيث أصدروا بيانا صحافيا معلقين فقط على تشويه موقع الويب الخاص بهم. رد القراصنة الصاع، ناشرين مقطع فيديو على يوتيوب YouTube يعرض شاشة حاسوب يظهر عليها ما بدا أنه آلاف من الملفات والمجلدات الخاصة بمؤسسة «ساندز»، بما فيها كلمات المرور وسجلات الائتمان الخاصة بنادي القمار، مع مربع نص مكتوب فيه: «هل تظن حقا أنه لم يُطَحْ إلا بمخدم البريد الخاص بك؟! إنه بالتأكيد قد تم!».

في غضون بضع ساعات، أزال مكتب التحقيقات الفدرالي الفيديو من موقع يوتيوب، وتمكنت الشركة من سحق مزيد من الفضائح، حتى قرب نهاية العام، حينما نشرت مجلة الأعمال الأمريكية الأسبوعية «بلومبيرغ بيزنس ويك» Bloomberg Businessweek تقريرا مطولا يوضح التفاصيل الكاملة للهجوم وأضراره. لكن التقرير لم يلفت الانتباه كثيرا، لأنه قبل ذلك بأسبوعين ضرب هجوم مماثل - كان أكثر تدميرا بكثير - عالم هوليوود الغارقة في الشهرة، وبالتحديد ضرب أحد استوديوهاتها الرئيسية، وهو «سوني بيكتشرز إنترتينمنت» Sony Pictures Entertainment.

في صباح يوم الاثنين، 24 نوفمبر، اخترقت عصابة من قراصنة الحاسوب يطلقون على أنفسهم اسم «حُراس السلام» Guardians of Peace[2] شبكة «سوني بيكتشرز»، مدمرين ثلاثة آلاف حاسوب، وثمانمائة مخدم حاسوبي، وسرقوا أكثر من مائة تيرا بايت من البيانات، بما في ذلك رواتب المديرين التنفيذيين، ورسائل البريد الإلكتروني، والنسخ الرقمية من أفلام لم تصدر بعد، وأرقام الضمان الاجتماعي لنحو 47 ألفا من الممثلين، والمقاولين (المتعهدين)، والموظفين. سرعان ما جرى إرسال كثير من تلك البيانات إلى الصحافة الشعبية الصفراء الذين أعادوا طبعها بابتهاج، ثم أرسلت إلى الصحف الرئيسية.

جرى اختراق «سوني» قبل ذلك[3] مرتين في العام 2011 وحده، أدت إحدى الهجمتين إلى إيقاف تشغيل شبكة «بلاي ستيشن» PlayStation الخاصة بها لمدة ثلاثة وعشرين يوما، بعد نهب بيانات من 77 مليون حساب مستخدم. خلال الاختراق الآخر سُرِقت بيانات من 25 مليون شخص من مشاهدي «سوني أونلاين إنترتينمنت» Sony Online Entertainment، بمن في ذلك اثنا عشر ألف رقم بطاقة ائتمان. بلغت التكلفة الناشئة عن الأعمال التجارية المفقودة[4]، والأضرار التي جرى إصلاحها، نحو 170 مليون دولار.

لكن، مثل العديد من التكتلات، كانت «سوني» تدير فروعها المختلفة بنمط المدخنة(*)، إذ لم يكن لدى المسؤولين التنفيذيين في «بلاي ستيشن» اتصال بهؤلاء في «أونلاين إنترتاينمنت»، الذين لم يكن لديهم أي علاقة بأولئك في «سوني بيكتشرز». لذلك، لم تكن الدروس المستفادة في أحد المجالات[5] يجري تشاركها مع الآخرين.

الآن، أدرك المسؤولون التنفيذيون أن عليهم أخذ الأمور على محمل الجد، ومن أجل طلب المساعدة في تعقب قراصنة الحاسوب وإصلاح الضرر، لم يتصلوا بمكتب التحقيقات الفدرالي فقط، لكنهم اتصلوا أيضا بشركة «فاير آي» FireEye، التي كانت قد اشترت أخيرا شركة «مانديانت» Mandiant، الشركة التي كان يترأسها «كيفين مانديا» Kevin Mandia - المحقق السابق في الجرائم السيبرانية في سلاح الجو، وكان أكثر ما اشتهرت به، أنها كشفت مجموعة واسعة من الهجمات السيبرانية التي شنتها الوحدة 61398 للجيش الصيني. سرعان ما توصلت «فاير آي»، بالاشتراك مع مكتب التحقيقات الفدرالي الذي كان يعمل مع وكالة الأمن القومي إلى تحديد المهاجمين على أنهم مجموعة تدعى «دارك سيول» (سيول المعتمة) DarkSeoul، التي كانت غالبا ما تضطلع بمهام سيبرانية لمصلحة حكومة كوريا الشمالية من بؤر استيطانية خارجية منتشرة في أنحاء آسيا.

كانت شركة «سوني بيكتشرز» قد خططت لإطلاق فيلم كوميدي بعنوان «المقابلة» The Interview في يوم عيد الميلاد (الكريسماس)، بطولة جيمس فرانكو

(*) «نمط المدخنة» stovepipe fashion: هو أن يكون هيكل المؤسسة يحد من تدفق المعلومات داخلها، أو يمنع الاتصال عبر المنظمات. ربما تتبنى منظمات الاستخبارات عمدا نمط المدخنة بحيث إذا حدث انتهاك أو فضح في أحد المواقع لا ينتشر إلى بقية المؤسسة. يستحضر هذا المصطلح صورة المداخن التي ترتفع فوق المباني، وكل منها يعمل بشكل فردي. [المترجم].

James Franco وسيث روغن Seth Rogen في دور مقدم برنامج حواري تلفزيوني هزلي ومنتجه المتورط في إحدى مؤامرات وكالة الاستخبارات المركزية لاغتيال حاكم كوريا الشمالية، كيم جونغ - أون Kim Jong-un. في يونيو السابق، حينما جرى الإعلان بشأن مشروع الفيلم، أصدرت حكومة كوريا الشمالية بيانا تحذر فيه من أنها «ستدمر بلا رحمة[6] كل من يجرؤ على إيذاء القيادة العليا للبلاد أو الهجوم عليها، حتى لو قليلا». بدا أن الاختراق كان إلحاقا للتهديد.

كان بعض اختصاصيي السيبرانية المستقلين يشككون في أن كوريا الشمالية هي التي كانت وراء الهجوم، ولكن أولئك المتعمقين داخل الأوساط الاستخباراتية للولايات المتحدة، كانوا على ثقة، على نحو غير معتاد. في العلن، كان المسؤولون الرسميون يقولون[7] إن قراصنة الحاسوب استخدموا كثيرا من «البصمات» ذاتها التي كانت مجموعة «دارك سيول» قد استخدمتها في الماضي[8]، بما في ذلك هجوم وقع قبل ذلك بعامين، وأطاح بأربعين ألف حاسوب في كوريا الجنوبية. لقد استخدموا الأسطر ذاتها من التعليمات البرمجية (الكود)، وخوارزميات التشفير، وأساليب محو البيانات، وعناوين بروتوكول الإنترنت IP addresses. لكن السبب الحقيقي[9] وراء يقين الحكومة تمثل في أن وكالة الأمن القومي كانت منذ فترة طويلة قد تغلغلت في شبكات كوريا الشمالية، كل ما يفعله قراصنتهم، كانت وكالة الأمن القومي تستطيع متابعته. وحينما كان قراصنة الحاسوب الكوريون يراقبون نتائج ما كانوا يفعلونه، كانت وكالة الأمن القومي تستطيع أن تعترض الإشارة من خلال شاشاتها - ليس في الوقت الفعلي (الحقيقي) (إلا إذا كان هناك سبب لمراقبة الكوريين الشماليين في الوقت الفعلي)، لكن كان محللو الوكالة يستطيعون استرجاع الملفات بأثر رجعي، ومشاهدة الصور، وتجميع الأدلة.

كانت هذه حالة أخرى لهجمة سيبرانية لم يجر إطلاقها من أجل المال، أو الأسرار التجارية، أو التجسس التقليدي، بل للتأثير في سلوك شركة خاصة.

نجح الابتزاز هذه المرة. قبل أسبوع واحد من يوم افتتاح فيلم «المقابلة»، تلقت «سوني» رسالة بريد إلكتروني تنطوي على تهديد باستخدام العنف ضد دور العرض التي تعرض الفيلم. ألغت «سوني» إطلاق الفيلم، وفجأة توقف تدفق رسائل البريد الإلكتروني والبيانات المحرجة إلى الصحف الشعبية الصفراء وإلى عالم المدونات.

لم يؤد خضوع الاستوديو إلا إلى تفاقم مشكلاتهم. في المؤتمر الصحافي الذي دأب الرئيس أوباما على أن يعقده في نهاية العام، قبل أن يطير إلى منزله في هاواي لقضاء العطلات، أخبر أوباما العالم بأن «سوني ارتكبت خطأ»[10] عندما ألغت الفيلم. واستطرد: «أنا أتمنى لو أنهم تحدثوا معي أولا. كنت سأقول لهم: لا تدخلوا في نمط يجري فيه ترهيبكم، بمثل تلك الأنواع من الأعمال الإجرامية». كما أعلن أن حكومة الولايات المتحدة سوف «ترد بشكل يتناسب» مع هجوم كوريا الشمالية «في المكان والزمان وبالطريقة التي نختارها».

كان البعض في العالم السيبراني في حيرة؛ فقد جرى اختراق مئات البنوك الأمريكية، وشركات البيع بالتجزئة، ومرافق عامة، ومقاولي الدفاع، وحتى شبكات وزارة الدفاع على نحو دوري، وأحيانا بتكلفة باهظة، ولم تتخذ حكومة الولايات المتحدة، من جانبها، أي إجراءات عقابية انتقامية، على الأقل ليس علنا. لكن يجري انتهاك استوديو في هوليوود، إزاء فيلم للسينما، ويتعهد الرئيس بالانتقام معلنا ذلك في مؤتمر صحافي متلفز؟

كان لدى أوباما وجهة نظر في إحداث هذا التمايز. في اليوم نفسه، قال جيه جونسون Jeh Johnson، وزير الأمن الداخلي، إن هجوم «سوني» لم يكن يشكل «مجرد هجوم[11] ضد شركة وموظفيها»، بل «هجوما أيضا على حريتنا في التعبير، وعلى نمط حياتنا». ربما يكون الفيلم الكوميدي الذي ينتجه روغن رمزا يصعب تصوره للتعديل الأول لدستور الولايات المتحدة الأمريكية والقيم الأمريكية، لكن كذلك كان كثير من الأعمال الأخرى التي تعرضت للهجوم عبر تاريخ الأمة، ومع ذلك ظلت تستحق الدفاع عنها؛ لأن الهجوم على القيم الأساسية كان لزاما التصدي له والرد عليه، مهما كان الهدف متواضعا وبسيطا، خشية أن يهدد بعض المعتدين في المستقبل بدهْم ملفات جهات أخرى، مثل: استوديو، أو ناشر، أو متحف فني، أو شركة تسجيل، إذا لم يلغ مسؤولوها التنفيذيون فيلما، أو كتابا، أو معرضا، أو ألبوما موسيقيا آخر.

أثار التصدي جدلا داخل البيت الأبيض، على غرار النقاشات التي دارت في ظل الرؤساء السابقين، لكن لم يجرِ حسمها قط، مثل: ما الرد الذي كان يتناسب مع هجوم سيبراني؟ هل ينبغي توجيه هذا الرد في الفضاء السيبراني؟ أخيرا، ما الدور الذي كان يجب على الحكومة أن تؤديه في التصدي للهجمات السيبرانية على المواطنين أو الشركات الخاصة؟ إذا تعرض أحد البنوك للاختراق، فإنها مشكلة البنك؛

لكن، ماذا لو اخْتُرِق بنكان، أو ثلاثة أو عشرة بنوك من البنوك الكبيرة؟ عند أي نقطة تصير تلك الاعتداءات مصدر قلق للأمن القومي؟

إنها كانت صيغة أرحب وأشمل من السؤال الذي كان روبرت غيتس قد طرحه على المحامي العام للبنتاغون قبل ذلك بثمانية أعوام، وهو: عند أي نقطة يشكل الهجوم السيبراني عملا من أعمال الحرب؟ لم يتلق غيتس قط أي رد واضح، ولم يزل الالتباس قائما منذ ذلك الحين.

في 22 ديسمبر[12]، بعد ثلاثة أيام من حديث أوباما في مؤتمره الصحافي بشأن اختراق شركة سوني، فصل بعضهم كوريا الشمالية عن شبكة الإنترنت. وجّه المتحدث باسم رئيس كوريا الشمالية كيم جونغ - أون Kim Jong-un الاتهام إلى واشنطن بشن الهجوم. إنه كان تخمينا منطقيا، إذ إن أوباما كان قد تعهد بإطلاق رد يتناسب مع الهجوم على «سوني»، وبدا أن إيقاف تشغيل شبكة الإنترنت في كوريا الشمالية مدة عشر ساعات يليق بهذا ويؤدي الغرض، وأنها لن تكون مهمة شاقة، نظرا إلى أنه لم يكن لدى الدولة كلها سوى 1024 عنوانا من عناوين بروتوكول الإنترنت Internet Protocol addresses (أقل من العدد الموجود في بعض أحياء مدينة نيويورك)، وجميعها متصل بالإنترنت من خلال مزود خدمة واحد في الصين.

في الحقيقة، على الرغم من ذلك، لم تؤدِ حكومة الولايات المتحدة أي دور في إيقاف التشغيل. نشب جدل في البيت الأبيض بشأن إنكار التهمة علنا. دفع البعض إلى أنه ربما يكون من الجيد توضيح ما الذي يعنيه الرد المتناسب. دفع آخرون إلى أن إصدار أي بيان كان سيشكل سابقة محرجة، إذ إنه إذا أصدر مسؤولون رسميون بالولايات المتحدة إنكارا الآن، ومن ثم يصير لزاما عليهم أن يصدروا إنكارا أيضا في المرة المقبلة التي تحدث فيها كارثة رقمية في أثناء المواجهة. خلاف ذلك كان الجميع سيستنبط أن أمريكا هي التي شنت ذلك الهجوم، سواء كانت هي التي قامت بذلك أو لا، عند هذه النقطة ربما يرد الضحية على الاعتداء(*).

(*) كحل توافقي، عندما أصدر أوباما في 2 يناير من العام 2015 أمرا تنفيذيا بفرض عقوبات جديدة ضد كوريا الشمالية، وصفه المتحدث باسم البيت الأبيض جوش إيرنست Josh Earnest بشكل واضح أنه «الطلعة الأولى من ردنا»[13] على اختراق «سوني». كان يمكن أن يستنبط المستمعون من كلمة «الأولى» أن الولايات المتحدة لم تكن قد أوقفت تشغيل الإنترنت في كوريا الشمالية قبل ذلك بأحد عشر يوما. لكن لم يعلن أي مسؤول ذلك صراحة، على الأقل ليس مدرجا في السجلات بشكل رسمي.

في هذه الواقعة، لم يصعّد الكوريون الشماليون النزاع، لأنهم جزئيا لم يكن في استطاعتهم ذلك. لكن قوة أخرى، مع إنترنت أكثر فعالية، ربما يكون في استطاعتها.

كان سؤال غيتس أصوب أكثر من أي وقت مضى، لكنه كان أيضا، جانبيا وخارج الموضوع بعض الشيء. حدث الهجوم السيبراني بسرعة خاطفة، واكتنف بدايته التباس وغموض لمصدره؛ لذلك، كان يمكن أن يستفز هجوما مضادا ربما يتصاعد إلى حرب، في الفضاء السيبراني وفي فضاء الواقع، بغض النظر عن نوايا أو مقاصد أي أحد.

في نهاية فترة رئاسة بوش وبداية فترة رئاسة أوباما، في أثناء حوارات غيتس العرضية غير الرسمية مع معاونيه وزملائه في البنتاغون والبيت الأبيض، أخذ يفكر مليا في مسائل أوسع نطاقا بشأن التجسس السيبراني والحرب السيبرانية.

في هذه المناسبات، كان سيقول: «نحن شاردون في منطقة معتمة».

كانت عبارة من طفولة غيتس في ولاية كانساس Kansas، حيث كان جده طوال نحو خمسين عاما يعمل مسؤول محطة (ناظر المحطة) في سكك حديد «سانتا في». كانت «المنطقة المعتمة» هي مصطلح الصناعة الذي يُطلق على ذلك النطاق من مسار السكة الحديد الذي لم يكن خاضعا للمراقبة بواسطة الإشارات. كان هذا الأمر بالنسبة إلى غيتس مناظرا تماما للفضاء السيبراني، باستثناء أن هذه المنطقة الجديدة كانت أكثر اتساعا وأشد خطرا، لأن المهندسين كانوا غير معروفين، وكانت القطارات غير مرئية، وكان التصادم يمكن أن يسبب مزيدا من الضرر.

حتى في أثناء أحلك أيام الحرب الباردة، كان غيتس سيخبر زملاءه بأن الولايات المتحدة والاتحاد السوفييتي وضعا واتبعا بعض القواعد الأساسية؛ على سبيل المثال، الاتفاق على عدم قتل إحدى الدولتين جواسيس الأخرى. لكن اليوم، في الفضاء السيبراني، لم يكن هناك مثل هذه القواعد، ولا أي قواعد من أي نوع. اقترح غيتس عقد اجتماع مغلق مع القوى السيبرانية العظمى الأخرى - الروس، والصينيين، والبريطانيين، والإسرائيليين، والفرنسيين - للتوصل إلى بعض المبادئ، بعض «القواعد التوجيهية» التي ربما تبدد نقاط ضعفنا الأمنية المتبادلة؛ لنقل، على سبيل المثال، اتفاق على عدم ابتداء هجمات سيبرانية على شبكات الحواسيب التي تتحكم في السدود، والمحطات المائية، وشبكات الطاقة الكهربائية، وتنظيم الملاحة الجوية، أي البنى الأساسية الحرجة المدنية، من الممكن استثناء فترة الحرب، وربما ليس حتى في فترة الحرب.

أولئك الذين سمعوا حدة نبرة صوت غيتس[14] كانوا يقطبون جباههم ويومئون برؤوسهم بوقار وقلق بالغ دلالة على الموافقة؛ لكن، لم يتبعه أحد، وذهبت الفكرة إلى المجهول.

على مدار الأعوام القليلة اللاحقة، اتسعت حدود هذه المنطقة المعتمة، وتضخمت حركة البيانات.

في العام 2014، كان هناك نحو[15] ثمانين ألف خرق أمني في الولايات المتحدة، أسفر أكثر من ألفين منها عن فقدان بيانات، بزيادة في عدد الخروقات بمقدار الربع، وزيادة في فقدان البيانات بمقدار 55 في المائة، مقارنة بالعام السابق. في المتوسط، كان قراصنة الحاسوب يمكثون فترة 205 أيام داخل[16] الشبكات التي انتهكوها، أي ما يقرب من سبعة أشهر، قبل أن يُكتشفوا.

كان من المرجح أن تحلّق تلك الأرقام عاليا وتسجل ارتفاعا كبيرا مع ظهور وتصاعد إنترنت الأشياء Internet of Things. في السابق في العام 1996 كان مات ديفوست، عالم الحاسوب الذي حاكى الهجمات السيبرانية في المناورات الحربية لحلف شمال الأطلسي (ناتو)، مشاركا في كتابة بحث بعنوان «الإرهاب المعلوماتي: هل يمكنك أن تثق بمحمصة الخبز خاصتك؟» Information Terrorism: Can You Trust Your Toaster?، كان العنوان طريفا بعض الشيء، لكن بعد مضي عشرين عاما، فإن معظم العناصر الدنيوية البسيطة في الحياة اليومية – محامص الخبز toasters، والبرادات (الثلاجات) refrigerators، ومنظمات الحرارة (الثرموستات) thermostats، والسيارات – باتت لها منافذ وأجهزة مودم للاتصال بالشبكة (ومن ثم لقراصنة الحاسوب أيضا)، بدا البحث استشرافيا وعالما بالمستقبل(*).

(*) في العام 2013، كان باحثان في الشؤون الأمنية[17] - أحدهما هو تشارلي ميللر Charlie Miller، وهو موظف سابق في «مكتب عمليات الولوج المصممة وفقا للحاجة» (تاو - تي إيه أوو)، الوحدة النخبوية للقرصنة الحاسوبية التابعة لوكالة الأمن القومي، قد اخترقا نظام الحاسب الخاص بالسيارة «تويوتا بريوس» Toyota Prius والسيارة «فورد إسكيب» Ford Escape، ثم عطلا المكابح وسيطرا على عجلة القيادة فيما كانت السيارات تُقاد في أرجاء ساحة لانتظار السيارات. في ذلك الاختبار، كان الباحثان قد وصّلا حواسيبهم سلكيا إلى المنافذ التشخيصية الموجودة على متن السيارات، والتي كانت مراكز الخدمة تستطيع الوصول إليها عبر الإنترنت. بعد مضي عامين، سيطرا لاسلكيا على سيارة «جيب شيروكي» Jeep Cherokee، بعد اكتشاف كثير من نقاط الضعف والثغرات الأمنية في الحواسيب الموجودة على متن السيارة - والتي اخترقاها أيضا لاسلكيا، من خلال وصلات البيانات ←

حاول الرئيس أوباما كبح الطوفان. في 12 فبراير من العام 2015 وقّع على أمر تنفيذي بعنوان «تحسين الأمن السيبراني للبنية الأساسية الحرجة»، لإنشاء منتديات تستطيع الشركات الخاصة من خلالها أن تتشارك بعضها مع بعض ومع الدوائر الحكومية، بيانات بشأن قراصنة الحاسوب في أوساطهم. في المقابل، فإن الدوائر الحكومية - لاسيما وكالة الأمن القومي، التي كانت تعمل من خلال مكتب التحقيقات الفدرالي – كانت ستقدم أدوات وتقنيات مصنفة على أنها سرية جدا لحماية شبكاتهم من الاعتداءات في المستقبل.

كانت تلك المنتديات نسخا أكبر وأقوى لمراكز تشارك وتحليل المعلومات التي كان ريتشارد كلارك قد أسسها في أثناء إدارة كلينتون، وكانت منكوبة وتعاني ذات الوهن، إذ إن كليهما كان طوعا؛ لم يكن تشارك المعلومات لزاما على مديري الشركات إذا لم يرغبوا في ذلك. أوضح أوباما هذه النقطة صراحة، ووفق ما نصت وثيقته: «لا شيء في هذا الأمر[18] يجوز تأويله لإعطاء دائرة سلطة التنظيم الرقابي لأمن البنية الأساسية الحرجة».

كانت اللوائح لاتزال أكبر مخاوف قطاع الصناعة الخاص، أكبر من خشيتهم من فقدان ملايين الدولارات على أيدي مجرمي أو جواسيس السيبرانية. مثلما كان زاتكو (مادج) بيتر، قرصان الحاسوب الأخلاقي (من ذوي القبعات البيضاء)، قد أوضح لديك كلارك قبل ذلك بخمسة عشر عاما، أن هؤلاء المديرين التنفيذيين كانوا قد احتسبوا أن تنظيف ما بعد هجوم سيبراني لا يكلف أكثر مما يكلف منع الهجوم ابتداء، وربما لا تنجح التدابير الوقائية بأي حال.

كانت بعض الصناعات قد غيرت حساباتها في الأعوام الفاصلة، لاسيما القطاع المالي الذي كانت أعماله تتمثل في جلب المال وبناء الثقة؛ وكان قراصنة الحاسوب

← عبر الإنترنت، والقنوات الخليوية، والأقمار الاصطناعية - بينما كان كاتب في مجلة «وايرد» Wired يقود السيارة على الطريق السريع. استدعت «فيات كرايسلر» Fiat Chrysler، مصنع السيارة «جيب شيروكي»، 1.4 مليون سيارة، لكن ميللر أوضح أن معظم السيارات الحديثة، ربما جميعها، يحتمل عدم حصانتها وربما تكون عرضة للهجوم بطرق مشابهة (على الرغم من عدم استدعاء أي منها). مثلما هي الحال مع معظم الأجهزة الأخرى في الحياة، كانت وظائفها الأساسية قد صارت محوسبة - والحواسيب متصلة بشبكات - من أجل تيسير استعمالها، أغفل مصنعوها الأخطار التي كانوا يفتحون الأبواب أمامها. إن علامات اتجاه جديد في سباق التسلح السيبراني – بما في ذلك التخريب، والفوضى، والإرهاب، وحتى مؤامرات الاغتيال، تُنفذ على نحو خفي أكثر من غارات الطائرات المسيرة من دون طيار - بدت مشؤومة ونذير سوء، ومحتومة تقريبا.

قد تسببوا في إحداث تقلص هائل في كليهما، وأدى تشارك المعلومات إلى الحد من الأخطار بشكل واضح. لكن البنوك الكبرى كانت استثناء من هذا النمط.

في وقت سابق، كان معاونو أوباما لشؤون السياسات السيبرانية قد قطعوا شوطا في إعداد مسودة للمعايير الأمنية الإلزامية، لكنهم سرعان ما تراجعوا. كانت ممانعة المؤسسات متصلبة جدا. ودفع وزيرا الخزانة والتجارة بأن من شأن اللوائح المتشددة إعاقة التعافي الاقتصادي، الاهتمام الأول لرئيس يعمل على انتشال البلاد من أعمق موجة كساد تمر بها على مدار سبعين عاما. إلى جانب ذلك، كان لدى المديرين التنفيذيين وجهة نظر، إذ إن المؤسسات التي كانت قد اعتمدت وتبنت معايير أمنية مشددة، كانت لاتزال تعاني الاختراق. كانت الحكومة قد قدمت أدوات، وتقنيات، وقائمة تضم «أفضل الممارسات»، لكن «أفضل» لم تكن تعني الكمال - بعد أن يتلاءم قراصنة الحاسوب، ربما أفضل الممارسات السابقة لا تكون حتى جيدة - وعلى أي حال، كانت الأدوات هي أدوات فقط، إنها لم تكن حلولا.

قبل ذلك بعامين، في يناير من العام 2013، كان فريق عمل مجلس علوم الدفاع قد أصدر تقريرا يتألف من 138 صفحة بشأن «التهديد السيبراني المتقدم»، وهو نتاج دراسة استغرقت ثمانية عشر شهرا، واستندت إلى أكثر من خمسين جلسة إحاطة مع الدوائر الحكومية، والقيادات العسكرية، والشركات الخاصة. خلص التقرير إلى أنه لم يكن هناك دفاع يعوّل عليه للتصدي لمهاجم سيبراني متخصص واسع الحيلة ومتفانٍ يبذل أقصى الجهد.

كان فريق عمل مجلس علوم الدفاع قد استعرض التدريبات والمناورات الحربية التي جرت أخيرا، وفي معظمها كان الفريق الأحمر «دائما» ينفذ حتى إلى شبكات وزارة الدفاع، و«يعرقل أو يهزم كلية»[19] الفريق الأزرق، باستخدام إكسبلويت(*) exploits كان يمكن لأي من قراصنة الحاسوب المحنكين تنزيلها من خلال الإنترنت.

كانت النتائج كلها تعيد إلى الأذهان تدريب «المتلقِّي المؤهَّل»، اعتداء الفريق الأحمر التابع لوكالة الأمن القومي في العام 1997 الذي كشف لأول مرة عن نقاط ضعف جيش الولايات المتحدة وثغراته الأمنية المشينة.

(*) «إكسبلويت» exploit، هي أداة برمجية مصممة للاستفادة من وجود عيوب في منظومة حاسوبية، وعادة يكون لأغراض ضارة مثل تنصيب البرامج الخبيثة. [المترجم].

كان بعض من أعضاء فريق عمل مجلس علوم الدفاع[20] قد شهد من كثب بداية تاريخ تلك التهديدات، من بينهم بيل ستوديمان، مدير وكالة الأمن القومي في أواخر الثمانينيات وأوائل التسعينيات من القرن العشرين، وهو أول من حذّر من أن الأطباق اللاقطة الراديوية والهوائيات الخاصة بالوكالة كانت «في طريقها إلى الصمم» وسط الانتقال العالمي من التناظرية (التماثلية) إلى الرقمية؛ وبوب جورلي Bob Gourley، أحد تلاميذ ستوديمان، أول رئيس استخبارات لفريق العمل المشترك لحماية شبكات الحاسوب التابع للبنتاغون، الذي تعقب اختراق «متاهة ضوء القمر» وعزاه إلى روسيا؛ وريتشارد شيفر، المدير السابق لمديرية ضمان المعلومات في وكالة الأمن القومي، الذي اكتشف أول نفاذ معروف لشبكة جيش الولايات المتحدة المصنفة على أنها سرية، مما دفع إلى عملية «اليانكي صائد الظباء» Buckshot Yankee.

من خلال حضورهم جلسات الإحاطة، وتجميع وتبويب استنتاجاتهم، وكتابة التقرير، شعر هؤلاء المحاربون المحنكون في الحروب السيبرانية الماضية – الحقيقي منها والذي على سبيل المحاكاة - كأنهم كانوا قد دخلوا إلى آلة الزمن؛ إذ إن القضايا، والتهديدات، والأكثر إثارة للدهشة نقاط الضعف والثغرات الأمنية، كانت هي ذاتها ما كانوا عليه قبل كل تلك الأعوام السابقة. كانت الحكومة قد أدخلت أنظمة وبرمجيات جديدة، وأنشأت دوائر ومديريات جديدة، لاكتشاف الهجمات السيبرانية والتصدي لها؛ لكن، مثلما هي الحال مع أي سباق تسلح آخر، فإن المتعدي - في الداخل والخارج – هو أيضا كان قد ابتكر واستنبط أدوات وتقنيات جديدة؛ وفي هذا السباق، كان المتعدي يتمتع بالأفضلية ويستحوذ عليها.

لاحظ التقرير أن «الربط الشبكي[21] الذي كانت الولايات المتحدة تستخدمه من أجل تحقيق أفضلية اقتصادية وعسكرية هائلة على مدار الأعوام العشرين السابقة، جعل البلاد غير حصينة، وعرضة للهجمات السيبرانية أكثر من أي وقت مضى». إنه كان ذات التناقض اللغز الذي كانت اللجان السابقة التي لا حصر لها قد لاحظته.

وفقا لما كتب أعضاء اللجنة، كانت المشكلة الأساسية التي لا مفر منها هي أن شبكات الحاسوب «أنشئت على بنى هي أصلا بطبيعتها متقلقلة وغير آمنة»[22]. كانت الكلمة الدليلية الرئيسية هنا هي أصلا بطبيعتها.

إنها كانت المشكلة التي كان ويليز واير قد أبرزها وأشار إليها قبل ذلك بنصف قرن تقريبا، في العام 1967، قبيل تعميم «أربانت» ARPANET، إذ إن وجود شبكة الحاسوب في حد ذاته، حيث كان يستطيع مستخدمون عدة الوصول إلى الملفات والبيانات على نحو فوري ودائم online من مواضع بعيدة وغير مأمونة، أنشأ مواضع ضعف وثغرات أمنية متأصلة.

لم يكن الخطر - كما رآه فريق العمل في العام 2013 - أن أحدا سيطلق من العدم وعلى نحو مفاجئ هجوما سيبرانيا على الآلة العسكرية الأمريكية أو البنية الأساسية الحرجة. إن الخطر بالأحرى تمثل في أن الهجمات السيبرانية كانت ستصير عنصرا في كل النزاعات المستقبلية. ونظرا إلى اعتماد جيش الولايات المتحدة على الحواسيب في كل شيء؛ بدءا من أنظمة توجيه الصواريخ باستخدام نظام تحديد المواقع (جي بي إس Global Positioning System (GPS)، إلى نظم الاتصالات في مراكز القيادة ومحطات الطاقة التي كانت تولد الكهرباء اللازمة لها، إلى أوامر الجدولة لإعادة تزويد القوات بالذخيرة، والوقود، والطعام، والماء. لذا، لم يكن هناك أي ضمان بأن أمريكا كانت ستكسب هذه الحرب. وذكر التقرير أنه «مع القدرات والتكنولوجيا الحالية[23]، فإنه من غير المحتمل الحماية بثقة لصد الهجمات السيبرانية الأكثر تطورا».

إن دفاعات سور الصين العظيم كان يمكن القفز فوقها أو الالتفاف حولها. بدلا من ذلك، خلص التقرير إلى أن فرق الأمن السيبراني، المدنية والعسكرية، كان يتعين أن ينصبّ تركيزها على الاكتشاف والقدرة على التحمل والصمود للتحايل على العطل، أي تصميم نظم يمكنها استطلاع الهجوم في وقت مبكر، وإصلاح الأضرار سريعا.

مع ذلك، كان سيظل الأكثر فائدة هو اكتشاف سبل لردع الخصوم ومنعهم من الاعتداء حتى في أكثر الأحوال إغواء.

لقد كان هذا هو المعضلة الكبرى في أوائل عهد الأسلحة النووية، حينما أدرك الخبراء الاستراتيجيون أن القنبلة الذرية - وفي وقت لاحق، القنبلة الهيدروجينية - كانت أكثر تدميرا مما كان يمكن أن يبرره هدف أي حرب. مثلما وضعها برنارد برودي Bernard Brodie - أول خبير استراتيجي في مجال الأسلحة النووية - في كتابه الذي نُشر بعد أشهر فقط من «هيروشيما» Hiroshima و«ناجازاكي»

Nagasaki بعنوان «السلاح الحاسم» The Absolute Weapon، «حتى ذلك الحين كان الغرض الرئيسي[24] لمؤسستنا العسكرية هو كسب الحروب. من الآن فصاعدا، يجب أن يكون غرضها الرئيسي هو تفادي الحروب». برر برودي ذلك على أنه حماية للترسانة النووية، بحيث إنه في حالة وقوع ضربة سوفييتية أولى، سيكون متبقيا لدى الولايات المتحدة ما يكفي من القنابل من أجل «الثأر المماثل».

لكن ما الذي كان يعنيه ذلك في الفضاء السيبراني الحديث؟ إن الدول التي ينظر إليها الكثيرون على أنها خصوم محتملون في مثل هذه الحرب، مثل: روسيا، والصين، وكوريا الشمالية، وإيران، لم تكن متصلة بالإنترنت بالقدر نفسه الذي وصلت إليه أمريكا، أو حتى ما يقرب منه. كان الثأر المماثل سيلحق بتلك الدول أضرارا تقل كثيرا عما كانت الضربة الأولى ستلحقه بأمريكا؛ من ثم، فإن أرجحية الثأر ربما لا تردعهم عن الهجوم. إذن ماذا كانت صيغة الردع السيبراني، التهديد بالرد على هجوم بإعلان حرب شاملة، إطلاق قذائف وقنابل ذكية، التصعيد إلى انتقام نووي؟ ثم ماذا؟

الحقيقة هي أنه لم يكن أحد في موضع السلطة أو من ذوي النفوذ رفيع المستوى قد فكر في هذا.

كان مايك ماكونيل قد تأمل المسألة في أثناء الفترة الانتقالية بين رئاستي بوش وأوباما، حينما أعد «المبادرة القومية الشاملة للأمن السيبراني» (سي إن سي آي). حددت المبادرة اثنتي عشرة مهمة لتُنجز في الأعوام القليلة اللاحقة، كان من بينها: تنصيب نظام عام لكشف التسلل عبر كل الشبكات الفدرالية، وتعزيز أمن الشبكات المصنفة على أنها سرية، وتعريف دور حكومة الولايات المتحدة في حماية البنية الأساسية الحرجة، وكانت هناك المهمة الرقم 10 في القائمة، وهي: «تعريف واستحداث[25] استراتيجيات وبرامج صلبة مستقرة».

شُكلت فرق من المعاونين والمحللين للعمل في المشروعات الاثني عشر. كان الفريق المكلف بالمهمة الرقم 10 لديه قصور ولم يصل إلى المطلوب، إذ إنه كتب بحثا، لكن أفكاره كانت غامضة وملتبسة جدا، وموجزة لدرجة يصعب معها وصفها بأنها «استراتيجيات»، فضلا عن كونها «برامج».

أدرك ماكونيل أن المسألة كانت صعبة جدا. كانت المهمات الأخرى هي أيضا صعبة، لكن في معظم تلك الحالات، كانت كيفية إنجاز المهمة واضحة إلى حد بعيد؛

للاحتيال على ذلك، جلب ماكونيل الأطراف الأساسية الحاسمة – الأجهزة الإدارية، والكونغرس، والقطاع الخاص، والصناعة – لتنفيذ المهمة. كان إدراك الردع السيبراني هو مشكلة مفاهيمية، أي من قراصنة الحاسوب هم الذين تحاول ردعهم؛ ما الذي تحاول ردعهم عن فعله؛ ما هي العقوبات التي تهدد بفرضها عليهم إذا ما هاجموهم على أي حال؛ وكيف ستتأكد من أنهم لن يهاجموا مجددا بضربة أقسى كرد فعل؟ كانت هذه أسئلة لصنّاع السياسة، وربما الفلاسفة السياسيين، وليس لأعضاء فريق العمل من المعاونين من المستوى الوظيفي الأوسط.

كان تقرير مجلس علوم الدفاع للعام 2013 قد تطرق قليلا إلى مسألة الردع السيبراني، مستشهدا بأوجه شبه مع ظهور القنبلة الذرية في نهاية الحرب العالمية الثانية. وأشار التقرير إلى أن «الأمر استغرق عقودا عدة[26] للتوصل إلى فهم وبلورة الاستراتيجيات التي تحقق توازنا مع الاتحاد السوفييتي». الكثير من هذا الفهم نشأ عن التحليلات وتدريبات الحرب في مؤسسة «راند»، بيت الخبرة الذي كان يرعاه سلاح الجو، حيث كان اقتصاديون، وفيزيائيون، وعلماء سياسة مدنيون - ومن بينهم برنارد برودي – يبتكرون ويختبرون أفكارا جديدة. كتب معدو التقرير من فريق العمل أنهم «لسوء الحظ لم يتمكنوا من العثور على أي دليل» على أن أي شخص، في أي مكان، كان يضطلع بهذا النوع من العمل «لفهم أفضل للحرب السيبرانية الواسعة النطاق».

بعد مضي عامين، في 10 فبراير 2015، بدأ أول الجهود الرسمية لإيجاد بعض إجابات بشأن هذه الأسئلة، مع الجلسة الافتتاحية لفريق آخر لمجلس علوم الدفاع، أُطلق على الفريق اسم «فريق العمل المعني بالردع السيبراني» (Task Force on Cyber Deterrence). كان الفريق سيعقد اجتماعاته في غرفة آمنة جدا في البنتاغون لمدة يومين كل شهر، وحتى نهاية العام. ووفقا للمذكرة التي بموجبها شُكِّل فريق العمل، كان هدفه هو «النظر في متطلبات[27] الردع الفعال للهجوم السيبراني ضد الولايات المتحدة والحلفاء أو الشركاء».

ضم أعضاء الفريق مجموعة مألوفة من قدامى الخبراء المحنكين في السيبرانية، من بينهم كريس إنجليس، نائب مدير وكالة الأمن القومي تحت إدارة كيث ألكسندر، وهو حاليا أستاذ (بروفيسور) الدراسات السيبرانية في الأكاديمية البحرية

للولايات المتحدة في أنابوليس Annapolis بولاية ماريلاند Maryland؛ وآرت موني، المسؤول السابق في البنتاغون الذي قاد سياسة الولايات المتحدة بشأن وسائل حرب المعلومات في أثناء حقبة التكوين الأولى في أواخر التسعينيات من القرن العشرين، وهو حاليا (وعلى مدار العقد السابق) رئيس المجلس الاستشاري لوكالة الأمن القومي؛ وميليسا هاثاواي، التي كانت سابقا مديرا للمشروعات في مؤسسة «بووز آلين»، والتي أحضرها مايك ماكونيل إلى البيت الأبيض لإدارة «المبادرة القومية الشاملة للأمن السيبراني» (سي إن سي آي)، وهي حاليا رئيس شركة استشارات خاصة بها؛ وروبرت باتلر Robert Butler، وهو ضابط سابق في مركز سلاح الجو لوسائل حرب المعلومات، الذي كان قد ساعد على إدارة أول محاولة عصرية لوسائل حرب المعلومات، الحملة ضد الرئيس الصربي سلوبودان ميلوسيفيتش وأتباعه. كان رئيس فريق العمل هو جيمس ميللر James Miller، وكيل وزارة الدفاع لشؤون السياسة، الذي عمل في قضايا السيبرانية في البنتاغون طوال أكثر من خمسة عشر عاما.

كان جميعهم على مدى فترة طويلة عناصر فاعلين في لعبة مقصورة فقط على من هم بداخل النظام؛ وبناء على وجودهم، يمكن الحكم بأن البيروقراطيين الراسخين في البنتاغون أرادوا أن تبقى الأمور على ما هي عليه.

في تلك الأثناء كانت السلطة والموارد تتركز في «فورت ميد»، حيث كانت القيادة السيبرانية للولايات المتحدة تحشد كتائبها، وتعد خطط المعركة، على الرغم من أن التساؤلات الواسعة المتعلقة بالسياسة والتوجيه كانت بالكاد قد طُرِحت، فضلا عن حسمها واستقرارها.

في العام 2011، حينما أدرك روبرت غيتس[28] أن وزارة الأمن الداخلي لن تكون قادرة على حماية البنية الأساسية الحرجة للبلاد من هجوم سيبراني (وبعد أن بدأت خطته للشراكة بين وزارة الأمن الداخلي ووكالة الأمن القومي تتلاشى كدخان)، أسند تلك المسؤولية أيضا إلى القيادة السيبرانية.

كانت مهمتا القيادة السيبرانية الأساسيتان الأصليتان أكثر وضوحا. المهمة الأولى، وهي دعم قادة الولايات المتحدة المقاتلين، كانت تعني استعراض خططهم الحربية ومعرفة الأهداف التي كان يمكن تدميرها بالوسائل السيبرانية بدلا من القذائف، والرصاص، والقنابل. أما المهمة الثانية، وهي حماية شبكات حاسوب وزارة الدفاع،

فكانت متوافقة تماما مع اهتمامات وقدرات «فورت ميد»، إذ إن تلك الشبكات كانت لها ثماني نقاط فقط للوصول إلى الإنترنت، وكانت القيادة السيبرانية تستطيع أن تعمل عليها جميعا، وتراقب المتسللين؛ وبطبيعة الحال، كان لديها أيضا السلطة السياسية والقانونية لرصد هذه الشبكات، والتجوال في داخلها.

لكن مهمتها الثالثة الجديدة، وهي حماية البنية الأساسية الحرجة المدنية، كانت مسألة أخرى. إن المؤسسات المالية، وشبكات الطاقة، وأنظمة النقل، والمنشآت المائية، وما إلى ذلك، كان لديها الآلاف من نقاط الوصول إلى الإنترنت، لم يكن أحد يعرف عددها على وجه الدقة، حتى إن كان جهاز الأمن القومي يستطيع أن يراقب هذه النقاط بطريقة ما، فإنه كان يفتقر إلى السلطة القانونية لفعل ذلك، ومن هنا جاء الأمر التنفيذي الذي أصدره أوباما، الذي اعتمد على القطاع الخاص بالصناعة لتشارك المعلومات طواعية، وهي أرجحية غير متوقعة، ولكنها الاختيار الوحيد المتاح.

كانت مفارقة مريرة موجعة. إن شرارة ازدهار هذا المجال برمته - أمن سيبراني، وتجسس سيبراني، وحرب سيبرانية - كانت قد اشتعلت قبل ذلك بثلاثين عاما، من جراء مخاوف بشأن أوجه الضعف وثغرات أمنية في البنية الأساسية الحرجة. مع ذلك بعد كل اللجان، والتحليلات، والأوامر التوجيهية، بدت المشكلة تستعصي على الحل.

مع ذلك لم يقبل كيث ألكسندر المهمة الجديدة فقط بل كان يجاهد من أجلها بشدة، كان قد ساعد غيتس على إعداد مسودة التوجيه التي أعطت المهمة للقيادة السيبرانية. في رأي ألكسندر فإن وزارة الأمن الداخلي لم تكن تفتقر إلى الموارد اللازمة لحماية الأمة فقط، بل كان لديهم خطأ مفاهيمي. كانت وزارة الأمن الداخلي تحاول تنصيب أنظمة كشف التسلل على كل الشبكات، وكانت هناك شبكات كثيرة جدا وسيكون من المستحيل رصدها، وكانت المحاولة ستكبد تكاليف باهظة. إلى جانب ذلك، ما الذي كان الجهاز الإداري في وزارة الأمن الداخلي يستطيع فعله إذا ما اكتشفوا هجوما خطيرا قيد التنفيذ؟

في رأي ألكسندر كان النهج الأصلح هو الشيء الذي كان يعرفه على أفضل وجه، اللجوء إلى الهجوم، أي الدخول إلى شبكات الخصم لكي تراه وهو يتهيأ

للهجوم، ثم تجعله ينحرف عن مساره. كان هذا هو المفهوم القديم لـ «الدفاع الإيجابي النشط»، أو في تجسيده السيبراني هو «استغلال شبكة الحاسوب» (سي إن إي)، والذي لم يكن يختلف كثيرا عن «مهاجمة شبكات الحاسوب» (سي إن أيه)، مثلما كان مديرو وكالة الأمن القومي الذين يعود تاريخهم إلى كين مينيهان ومايك هايدن على دراية جيدة بذلك.

لكن ألكسندر كان يؤيد مسارا آخر أيضا، تتمة ضرورية، وهي إجبار البنوك والقطاعات الأخرى - أو استمالتهم بحوافز مغرية – على تشارك المعلومات بشأن مخترقيهم مع الحكومة، وبكلمة «الحكومة»، كان ألكسندر يعني مكتب التحقيقات الفدرالي، ومن خلاله وكالة الأمن القومي والقيادة السيبرانية. هو قطعا لم يكن يعني وزارة الأمن الداخلي. وعلى الرغم من ذلك، وخلافا للبيت الأبيض الذي كان قد عين وزارة الأمن الداخلي على أنها الدائرة التي تقود حماية البنية الأساسية الحرجة، فإنه كان سيقول إن الوزارة كان يمكن أن تكون بمنزلة «جهاز التوجيه» (الراوتر router) الذي يرسل التحذيرات إلى دوائر أخرى أكثر فعالية.

كان ألكسندر مصرا على هذه النقطة. رفضت معظم الشركات الخاصة أن تتشارك المعلومات، ليس فقط لأنها كانت تفتقر إلى الحوافز، ولكن أيضا لأنها كانت تخشى الملاحقة القضائية، إذ إن بعض تلك المعلومات كانت ستتضمن بيانات شخصية عن الموظفين والعملاء. ردا على ذلك حث الرئيس أوباما الكونغرس على تمرير مشروع قانون يعفي الشركات من المسؤولية إذا تشاركوا البيانات. لكن ألكسندر عارض مشروع القانون، لأن نسخة أوباما من مشروع القانون كانت ستلزمهم بتشارك البيانات مع وزارة الأمن الداخلي. ومن دون إخطار البيت الأبيض حشد ألكسندر تأييد حلفائه في «كابيتول هيل» من أجل الضغط لتعديل مبادرة قائده الأعلى أو وأدها.

كانت خطوة حمقاء تفتقر إلى الحكمة، من شخص عادة ما كان أكثر اعتدالا ولباقة. أولا، سرعان ما سمع موظفو البيت الأبيض بشأن حشده للتأييد وممارسته للضغط، الأمر الذي جعله غير محبب لدى الرئيس، لاسيما في أعقاب تسريبات سنودن التي كانت قد مزقت بالفعل الأرصدة الاحتياطية لسمعة «فورت ميد» الطيبة وحسن ظن الشعب بها. ثانيا، إنها كانت هزيمة ذاتية من حيث المضمون

ومن منظور موضوعي، إذ إنه، حتى مع الإعفاء من المسؤولية، كانت الشركات تعزف عن إعطاء بيانات خاصة إلى الحكومة، ويصير الأمر أكثر صعوبة إذا عُرِّفت «الحكومة» على نحو صريح على أنها وكالة الأمن القومي.

من ثم كان مشروع قانون تشارك المعلومات معرضا للخطر، من قبل ائتلاف لا يبعث على التفاؤل، بين المدافعين عن الحريات المدنية، الذين كانوا من حيث المبدأ يعارضون تشارك البيانات مع الحكومة، والمؤيدين لوكالة الأمن القومي، الذين كانوا يعارضون تشارك البيانات مع أي كيان خلاف «فورت ميد».

لذا، كان الدفاع المنسق الوحيد الذي سيتبقى، هو «الدفاع الإيجابي النشط»، أي وسائل الحرب السيبرانية الهجومية.

كان هذا هو الوضع الذي ورثه الأدميرال مايكل روجرز Michael Rogers، وهو اختصاصي محترف في علم التشفير، الذي حل محل ألكسندر في أبريل 2014. كان روجرز قد تولى إدارة القيادة السيبرانية لأسطول سلاح البحرية، الذي كان مقره أيضا في «فورت ميد»، قبل أن يتولى قيادة وكالة الأمن القومي والقيادة السيبرانية للولايات المتحدة. وكان أيضا أول ضابط بحري يحصل على ثلاث نجوم (كان لديه حينئذ أربع نجمات) بعد أن ارتقى في الرتب كمخترق للشفرات. بعد فترة وجيزة من توليه القيادة، وفي مقابلة مع الخدمة الإخبارية للبنتاغون، سُئل عن الكيفية التي كان سيحمي بها البنية الأساسية الحرجة من اعتداء سيبراني - المهمة الثالثة للقيادة السيبرانية. أجاب روجرز بأن «التركيز الأكبر»[(29)] سيكون هو «محاولة اعتراض الهجوم لمنعه قبل أن يصل إلينا أساسا»؛ بعبارة أخرى، الوصول إلى داخل شبكة الخصم، من أجل رؤيته وهو يعد هجوما، ثم نعمل على انحراف مساره أو استباقه لمنعه من الهجوم.

استطرد روجرز قائلا: «إذا فشل ذلك»، كان «من المحتمل» أيضا «أنه سيعمل بشكل مباشر مع شبكات البنية الأساسية الحرجة تلك» التي «كان يمكن أن تكون لها قدرات دفاعية أقوى». لكنه كان يعلم أن هذا كان إجراء احتياطيا، وهو في ذلك الخصوص إجراء احتياطي واهٍ غير مرغوب فيه، لأنه لم يكن باستطاعة «فورت ميد» أو البنتاغون فعل الكثير من تلقاء نفسه من أجل دعم وتعزيز دفاعات القطاع الخاص.

في أبريل من العام 2015 أقرّت إدارة أوباما المنطق الأساسي، في وثيقة مؤلفة من ثلاث وثلاثين صفحة بعنوان «الاستراتيجية السيبرانية لوزارة الدفاع» (The Department of Defense Cyber Strategy)، التي وقّع عليها آشتون كارتر Ashton Carter، الفيزيائي الأمريكي والأستاذ السابق في جامعة هارفارد، وهو مسؤول رسمي في البنتاغون لفترة طويلة، ورابع وزير دفاع في عهد أوباما. في تلك الوثيقة، وبشيء من التفصيل، وُضِعت المهمات الثلاث ذاتها، وهي: مساعدة القيادات القتالية للولايات المتحدة، وحماية شبكات وزارة الدفاع، وحماية البنية الأساسية الحرجة. للاضطلاع بهذه المهمة الأخيرة نصت الوثيقة على أنه «بالاشتراك مع الدوائر الحكومية الأخرى»[30] (الكلمة التلطيفية والتعبير المجازي النمطي للتعبير عن وكالة الأمن القومي)، كانت وزارة الدفاع قد استحدثت «طائفة من الخيارات والأساليب لعرقلة الهجمات السيبرانية ذات العواقب الملموسة» قبل أن يكون لها تأثير. أضاف التقرير، في فقرة أكثر صراحة مما هو معتاد في التلميحات إلى خيار مهاجمة شبكة الحاسوب (سي إن إيه)، «إذا صدرت توجيهات إلى وزارة الدفاع كان لزاما عليها أن تكون قادرة على استخدام العمليات السيبرانية لزعزعة شبكات القيادة والسيطرة الخاصة بالخصوم، والبنية الأساسية الحرجة ذات الصلة بالنواحي العسكرية، وقدرات الأسلحة».

قبل ذلك بشهر، في 19 مارس، في جلسات الاستماع أمام لجنة مجلس الشيوخ المعنية بأفرع القوات المسلحة، أعرب الأدميرال روجرز عن المغزى على نحو أكثر مباشرة، قائلا إن ردع هجوم سيبراني يستلزم مجابهة ومناقشة السؤال: «كيف نزيد[31] قدرتنا على الجانب الهجومي؟».

سأل السيناتور جون ماكين John McCain، الجمهوري رئيس اللجنة، عما إذا كان صحيحا أن «مستوى الردع الحالي غير رادع».

أجاب روجرز: «هذا صحيح». إن المزيد من الردع السيبراني يعني المزيد من أدوات الهجوم السيبراني، والمزيد من الضباط المدربين على استخدامها، الأمر الذي كان يعني المزيد من المال والنفوذ للقيادة السيبرانية.

لكن هل كان هذا صحيحا؟؛ كان روجرز في جلسة استماع سابقة قد تصدر عناوين الأخبار بإدلائه بالشهادة بأن الصين «ومن المحتمل دولة أو دولتين[32]

أخريين» كانت بلا أدنى شك داخل الشبكات التي تتحكم في شبكات الكهرباء الأمريكية، والمنشآت المائية، وغيرها من الأصول المهمة الحساسة. لم يقل روجرز ذلك، لكن أمريكا كانت هي أيضا داخل الشبكات التي تتحكم في مثل هذه الأصول في تلك الدول الأخرى. هل كان الاختراق والتوغل على نحو أكثر عمقا سيحول دون الهجوم، أم أنه - في حالة حدوث أزمة - كان فقط سيغري الطرفين، وكل الأطراف، على مهاجمة شبكات الأطراف الأخرى على نحو استباقي، قبل أن تهاجم الأطراف الأخرى شبكاتهم أولا؟ وحالما يبدأ تبادل الهجمات، كيف كان سيمكن لأي شخص أن يمنعهم من التصعيد إلى مزيد من الضربات السيبرانية المدمرة، أو إلى حرب شاملة؟

كانت هذه تساؤلات حاول البعض الإجابة عنها، لكن لم يسبق لأحد أن توصل إلى إجابة في أثناء الجدال والمداولات والألاعيب النووية التي دارت في أثناء الحرب الباردة. لكن بينما كانت الأسلحة النووية أكثر تدميرا على نحو لا مثيل له، كان هناك أربعة اختلافات بشأن سباق التسلح الجديد هذا، الأمر الذي جعله أكثر احتمالا لأن يجنح خارج نطاق السيطرة. أولا، إنه يتضمن أكثر من اثنين من العناصر الفاعلة، بعضها يتعذر التنبؤ به، وبعضها لم يكن حتى دولا قومية. ثانيا، سيكون الهجوم غير مرئي، وفي بادئ الأمر يصعب تتبعه، مما يعزز فرص الحسابات الخاطئة وسوء التقدير من جانب البلد الذي ضرب أولا. ثالثا، هناك جدار حماية واضح وسميك يفصل بين استخدام الأسلحة النووية وعدم استخدامها، فالدول التي كانت تمتلك الأسلحة كانت مقيدة من استخدامها لأنه، من جانب، لم يكن أحد يعرف مدى الغضب وسرعة تصاعد العنف بمجرد انهيار الجدار الواقي. في المقابل فإن الهجمات السيبرانية كانت بشكل أو بآخر أمرا شائعا معتادا، إذ إنها كانت تندلع أكثر من مائتي مرة في اليوم ولم يكن أحد يعرف، لم يكن أحد قد أعلن من قبل مطلقا، لم يكن أحد قادرا على التنبؤ أين يمكن رسم الخط الفاصل بين الخطر الجسيم وما هو مصدر إزعاج فقط؛ ومن ثم كانت هناك فرصة أكبر لأن يتخطى أحد الخط الفاصل، لربما كان من دون أن يقصد، أو أنه لم يكن حتى على دراية بوجوده.

ختاما، كان هناك التكتم الشديد المتطرف الذي يحيط بكل شيء بشأن الحرب السيبرانية. كانت بعض الأشياء بشأن الأسلحة النووية أيضا مصنفة على أنها سرية، مثل: تفاصيل تصميمها، ورموز (كود) الإطلاق، وخطط الاستهداف، وإجمالي المخزون

الاحتياطي من ترسانة المواد النووية. لكن الأساسيات كانت معروفة جيدا، مثل: تاريخها، وكيف كانت تعمل، وكم كان عددها، ومقدار الدمار الذي كان يمكن أن تحدثه، وهو ما يكفي لتيسير إجراء نقاش متحضر وحصيف، حتى إن كان بواسطة أناس ليست لديهم صلاحيات أمنية سرية جدا. لم يكن الأمر كذلك فيما يخص السيبرانية، إذ إن الأدميرال روجرز حينما أدلى بشهادته بأنه يرغب في «زيادة قدراتنا على الجانب الهجومي»، فإن عددا من أعضاء مجلس الشيوخ فقط هم الذين كان لديهم أدنى فكرة بسيطة عما كان يتحدث بشأنه.

في تقرير الرفاق الخمسة حول إصلاح وكالة الأمن القومي، الذي كلف بإجرائه الرئيس أوباما في العام 2013 في أعقاب ما كشف عنه سنودن، أقر معدو التقرير، بل إنهم حتى شددوا على الحاجة إلى الإبقاء على مصادر، وأساليب، وعمليات بعينها مصنفة على أنها سرية جدا. لكنهم أيضا اقتبسوا على نحو مقنع فقرة من تقرير السيناتور فرانك تشيرتش، الذي كتب إثر فضيحة استخباراتية أخرى وقعت قبل ذلك بأربعين عاما تقريبا، وكانت على نحو جلي غير مشروعة. أعلن تشيرتش: «كان ينبغي أن يعرف الشعب الأمريكي[33] ما يكفي بشأن الأنشطة الاستخباراتية، حتى يكونوا قادرين على إعمال حسن إدراكهم وحسهم السليم تجاه القضايا الأساسية الكامنة وراء السياسة والمبادئ الأخلاقية».

هذه المعرفة، التي أطلق السيناتور تشيرتش عليها اسم «مفتاح السيطرة» (the key to control)، كانت مُفتقَدة في نقاشات السياسة، والاستراتيجية، والمبادئ الأخلاقية في الحرب السيبرانية. نحن جميعا شاردون في منطقة معتمة، معظمنا لم يعرف بشأنها إلا حديثا فقط، وحتى الآن بصورة باهتة.

شكر وعرفان

خطرت لي فكرة هذا الكتاب - صِيغَ التعاقُد، وبَدَأتْ عملية البحث، وأجريت المقابلات الأولى مع المصادر - قبل أن يسمع العالم عن إدوارد سنودِن؛ وقبل دخول البيانات الواصفة، وبرنامج «بريزيم» PRISM، والتشفير إلى هزل الأحاديث العامة؛ وقبل أن تصير الهجمات السيبرانية - التي أطلقتها الصين، وروسيا، وكوريا الشمالية، وإيران، وجماعات الجريمة المنظمة، نعم، وحكومة الولايات المتحدة - مادة رئيسية للأخبار يوميا كما يبدو للناظر. كان مُقترحي هو كتابة تاريخ لما قد أضحى معروفا على نطاق واسع بأنه «الحرب السيبرانية»، وازداد اهتمامي بالفكرة

حينما تراكمت القصص عن سنودِن وما سرَّبه من آلاف الوثائق، لأنه كان جليا أن قِلَّة من الناس، حتى بين أولئك الذين درسوا الوثائق من كثب (أنا أظن أنه حتى بين أولئك الذين كتبوا عن الوثائق، وحتى سنودن ذاته) كانوا يعرفون أن هناك تاريخا، أو إذا عرفوا ذلك، فهم لا يعلمون أن هذا التاريخ لا يرجع إلى بضع سنوات، ولكن إلى خمسة عقود، إلى بدايات الإنترنت ذاتها.

يمكن اعتبار هذا الكتاب الثالثَ في سلسلة من الكتب التي قد كتبتها عن تفاعل السياسة والأفكار والشخصيات في الحرب الحديثة. كان الكتاب الأول بعنوان «سحرة هرمغدون» The Wizards of Armageddon (1983)، وكان يدور حول صفوة مُفكري مؤسسات الفكر الذين اخترعوا الاستراتيجية النووية ونَسج مبادئها في السياسة الرسمية. كان الكتاب الثاني، «المتمردون» The Insurgents (2013)، عن صفوة مُفكري ضباط الجيش الميداني الذين أعادوا إحياء عقيدة مُكافحة التمرد، وحاولوا تطبيقها على الحروب في العراق وأفغانستان. الآن، يقتفي كتاب «المنطقة المُعتمة» Dark Territory أثر العناصر الفاعلة والأفكار والتقنيات المتعلقة بالحروب السيبرانية التي تلوح في الأفق.

في الكتب الثلاثة، كان ليّ حظ عظيم بأن عملت مع أَلِيس مايهيو Alice Mayhew، المُحرِّرة الأسطورية في مؤسسة «سايمون آند شوستر» Simon & Schuster، وأنا مدين لها بوجود تلك الكتب. بذور هذا الكتاب غُرست في أثناء مُحادثة في مكتبها، إما في ديسمبر 2012، وإما في يناير 2013 (قبل أو بعد نشر كتاب «المتمردون» The Insurgents)، حينما سألتني أَلِيس، في محاولة لدفعي إلى كتابة كتاب آخر، ما الموضوع المرجح أن يكون تاليا من بين الموضوعات الضخمة في المسائل العسكرية؟ أجبت على نحو مُبهم بأن «السيبرانية» ربما تكون جادة وخطيرة. سألتني مزيدا من الأسئلة؛ وأجبتها على نحو كامل قدر ما استطعت (لم أكن في ذلك الوقت أعرف حقا الكثير عن الموضوع). مع انتهاء الاجتماع، كنت التزمت بالنظر في أمر إعداد كتاب عن الحرب السيبرانية - أولا، لمعرفة ما إذا كانت هناك قصة، قصة تحتوي على شخوص ونابضة بما يُسرد، واتضح أنه يوجد.

أتوجه بالشكر إلى أَلِيس لحفزي في هذا الاتجاه، ولسؤالها أسئلة ثاقبة أخرى في كل خطوة على طول الطريق. أشكر كامل فريق المشروع بمؤسسة

«سايمون آند شوستر»Simon & Schuster، وهُم: ستيوارت روبرتس Stuart Roberts، وجاكي سيو Jackie Seow»، وجوناثان إيفانز Jonathan Evans، وستيفِن بيدفورد Stephen Bedford، ولاري هيوز Larry Hughes، وإلين ساساهرا Ellen Sasahara، وديفن نورمان Devan Norman، وبصفة خاصة الناشر جوناثان كارب Jonathan Karp. وأشكر فرِد تشايس Fred Chase على التنقيح اليقظ الدقيق. وأليكس كارب Alex Carp وجولي تايت Julie Tate على المثابرة في الفحص الدؤوب للحقائق (لكنني أتحمل المسؤولية كاملة عن أي أخطاء تبقى).

أتى دعم إضافي من «مجلس العلاقات الخارجية» Council on Foreign Relations، حيث كنت الزميل الصحافي لإدوارد مورو Edward R. Murrow خلال العام، حينما أجريت كثيرا من أبحاث الكتاب. على وجه الخصوص، أشكر قادة الزمالة جانين هيل Janine Hill وفيكتوريا أليكين Victoria Alekhine، ومساعدتي النشطة أثناء العام آليا ميديفبيكوفا Aliya Medetbekova، بالإضافة إلى العديد من زملاء المجلس، وهيئة مُتخصصيه، والمتحدثين الزائرين الذين كانت لي معهم حوارات وَقّادة مُلهمة (ينبغي أن أشدد على أنه لا المجلس ولا أي شخص في المجلس كان له أي دور في الكتاب ذاته، بما يتجاوز توفير غُرفة مكتب جيدة، وراتب، ومساعدة إدارية).

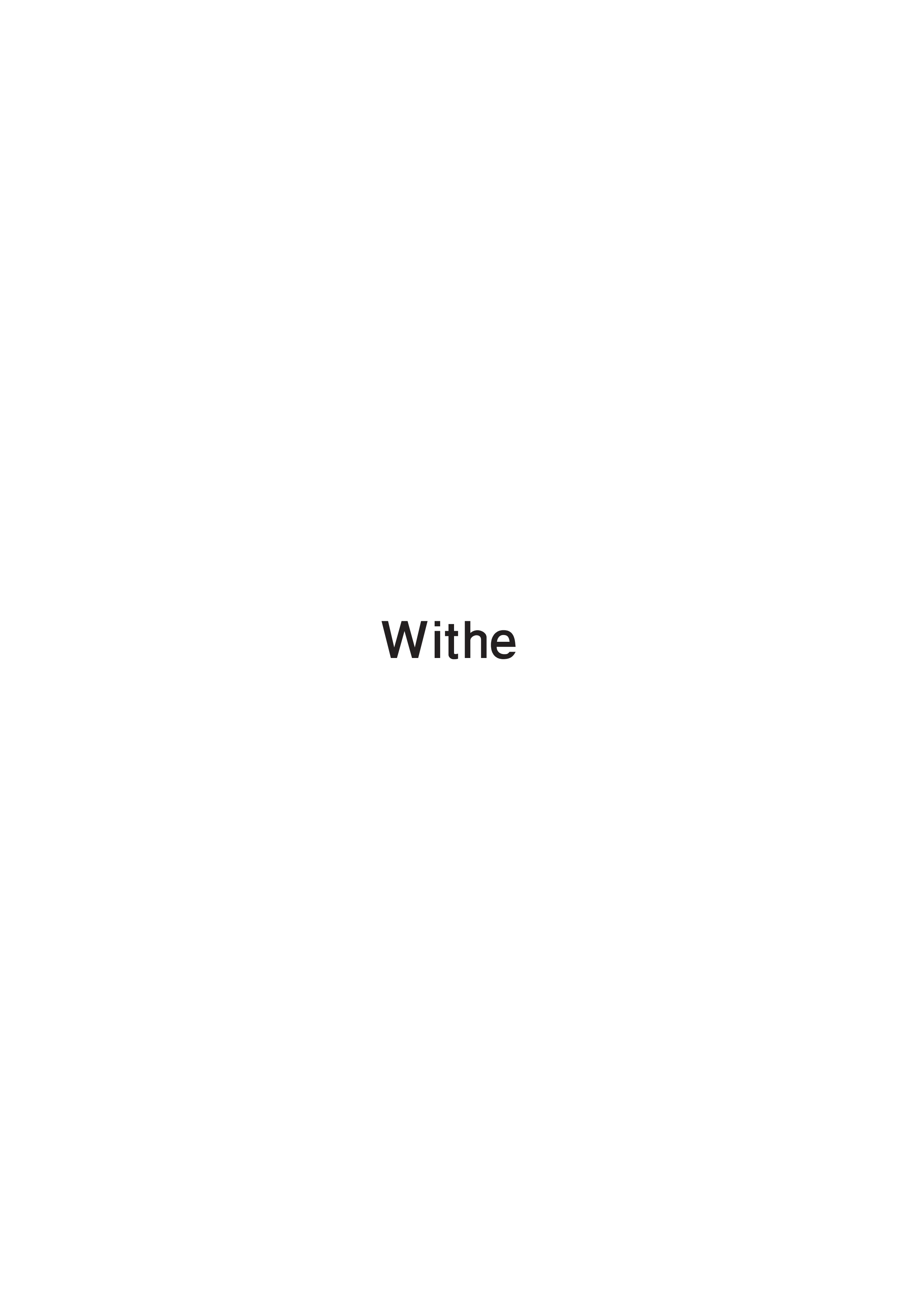
في إطار بحثي، أجريت مقابلات مع أكثر من مائة شخص ممن مارسوا دورا في هذه القصة، والعديد منهم التقيت معهم عدة مرات، مع متابعات بالبريد الإلكتروني والاتصالات الهاتفية. تباينت المقابلات فشملت وزراء، وجنرالات، وأدميرالات (بمن في ذلك ستة من مديري وكالة الأمن القومي)، واختصاصيين فنيين في الدهاليز الخفية للأجهزة الأمنية (وليس وكالة الأمن القومي فقط)، وكذلك الضباط، والمسؤولين الرسميين، والمعاونين، والمحلِّلين في كل منصب بينهم. أُجريت كل هذه المقابلات في سِريَّة؛ معظم المصادر لم توافق على التحدث معي سوى بهذا الشرط، لذا فأنا يجب أن أشير إلى أن معظم حقائق الكتاب (وكل الحقائق، حينما يتعلق الأمر بالإفصاحات الجديدة تاريخيا) تأتي من مصدرين على الأقل في مناصب مُطلعة. أشكر جميع هؤلاء الناس؛ من دونكم ما كان هذا الكتاب موجودا.

كما أشكر أيضا مايكل وارنر Michael Warner، المؤرخ الرسمي للقيادة السيبرانية للولايات المتحدة U.S. Cyber Command، وجيسون هيلي Jason Healey، وكارل غريندال Karl Grindal من جمعية دراسات الصراع السيبراني Cyber Conflict Studies Association، على حلقات النقاش ومجموعات الوثائق التي رُفعت عنها السرية، والتي كانت وسيلة فعَّالة في إقناعي - في مرحلة مبكرة من المشروع - بأن هناك قصة، وتاريخا، ليُقال هنا.

هذا هو كتابي الخامس على مدى ثلاثة وثلاثين عاما، وقد كان المرشد لها جميعا لترى النور هو وكيل أعمالي الأدبية رايف ساغالين Rafe Sagalyn الذي كان طوال الوقت سندا لي بوصفه مسؤولا، ومستشارا، وصديقا. أشكره مُجددا، بالإضافة إلى مساعديه الصبورين، براندون كوارد Brandon Coward وجيك ديباك Jake DeBache.

في النهاية، أنا ممتن لأصدقائي وعائلتي لتشجيعهم لي في نواحٍ عديدة. وأشكر على نحو خاص أمي روث كابلان بولوك Ruth Kaplan Pollock، التي طالما كانت تشد من أزري؛ وزوجتي برووك غلادستون Brooke Gladstone، التي قد بزغت منذ أن تجاوزنا بصعوبة سن المراهقة بوصفها صديقتي المفضلة، وحب حياتي، ومرشدتي للخصال الحميدة؛ وابنتينا، صوفي Sophie وماكسين Maxine، اللتين يُدهشني دائما إخلاصهما وحَمِيّتهما.

الهوامش



Withe

معظم ما تضمنه هذا الكتاب جاء نتيجة مقابلات أُجريت مع أكثر من مائة شخص ممن شاركوا في موضوعاته، وأعقبت الكثير منها رسائل وردت عبر البريد الإلكتروني، أو خلال مكالمات هاتفية، أو مقابلات شخصية متكررة. (للمزيد بشأن هذه المصادر، راجع قسم «شكر وعرفان»). وفي الهوامش الآتية لم أستشهد بمصادر المواد التي هي محض مقابلات فقط. أما المواد التي جاءت جزئيا من مصادر مكتوبة (كتب، ومقالات، ووثائق، وما إلى ذلك) وجزئيا من مقابلات، فقد استشهدت بها متبوعة بكلمة «ومقابلات».

الفصل الأول

(1) كان عرض تلك الليلة: خلال الأعوام الثمانية التي قضاها «ريغان» في منصبه رئيسا للبلاد، شاهد ريغان 374 فيلما في «كامب ديفيد» وفي قاعة العرض بالبيت الأبيض، بمعدل يبلغ نحو فيلم واحد في الأسبوع، وإن كانت عادته مشاهدة أكثر من ذلك العدد.
("Movies Watched at Camp David and White House," Aug. 19, 1988, 1st Lady Staff Office Papers, Ronald Reagan Library).
كان فيلم «ألعاب الحرب (المناورات الحربية) WarGames» اختيارا غير اعتيادي؛ كان ريغان عادة يشاهد أفلام مغامرات، أو كوميديا خفيفة، أو أفلاما موسيقية غنائية. لكن أحد كتاب سيناريو الفيلم، لورنس لاسكر Lawrence، كان ابن الممثلة جين جرير Jane Greer والمنتج إدوارد لاسكر Edward Lasker، وهما صديقان قديمان لريجان منذ أن كان نجما سينمائيا في هوليوود. استخدم لورنس اتصالاته العائلية للحصول على نسخة من الفيلم للرئيس. (مقابلات).

(2) في صباح يوم الأربعاء التالي:
Office of the President, Presidential Briefing Papers, Box 31, 06/08/1983 (case file 150708) (1), Ronald Reagan Library;
ومقابلات.
تم ذكر هذا الاجتماع في:
" Lou Cannon, President Reagan: The Role of a Lifetime (New York : Simon & Schuster, 1991), 38"
لكن، إضافة إلى أنه أخطأ في التاريخ، صوره كانون Cannon على أنه مجرد حالة سخيفة لاعقلانية أخرى لاتخاذ ريغان للأفلام بجدية بالغة، ولم يسرد كانون سؤال الرئيس للجنرال فيسي، ويبدو أنه لم يكن واعيا أن المشاهدة، وهذا الاجتماع الذي تلاها في البيت الأبيض، كان لهما تأثير في التاريخ. انظر أيضا:
Michael Warner, "Cybersecurity: A Pre-history," Intelligence and National Security, Oct. 2012.

(3) أشد ما تكون عرضة للاعتراض: منذ ذلك الحين رُفع الحظر عن التوجيه الرئاسي السري المتعلق بالأمن القومي (إن إس دي دي145- NSDD-145): http://fas.org/irp/offdocs/nsdd145.htm.

(4) تأسست وكالة الأمن القومي في العام 1952: مثلما دُونت لاحقا في الأمر التنفيذي الرقم 12333، الذي وقعه رونالد ريغان في 4 ديسمبر من العام 1981. ومُنعت وكالة الأمن القومي ومكتب التحقيقات الفدرالي من جمع معلومات استخباراتية أجنبية «لغرض الحصول على معلومات تتعلق بالأنشطة المحلية لأشخاص في الولايات المتحدة». وهذه العبارة الأخيرة تشير إلى المواطنين الأمريكيين، والمقيمين على نحو مشروع، والشركات

http://www.archives.gov/federal-register/codification/executive-order/12333.html.

(5) خلال الأعوام الثلاثة الأولى للقيادة السيبرانية:

Ellen Nakashima, "Pentagon to Boost Cybersecurity Force," Washington Post, Jan. 27, 2013؛

ومقابلات.

(6) في الحرب الأهلية الأمريكية:

Edward J. Glantz, "Guide to Civil War Intelligence," The Intelligencer: Journal of U.S. Intelligence Studies (Winter/Spring 2011), 57; Jason Healey, ed., A Fierce Domain:. Conflict in Cyberspace, 1986 to 2012 (Washington, D.C.: Atlantic Council, 2013), 27

(7) في أثناء الحرب العالمية الثانية: انظر بصفة خاصة

.David Kahn, The Codebreakers (New York: Scribner; rev. ed., 1996), Ch. 14

(8) رجل يدعى دونالد لثام Donald Latham:

Warner, "Cybersecurity: A Pre-history";

ومقابلات.

(9) في أبريل من العام 1967:

Willis H. Ware, Security and Privacy in Computer Systems (Santa Monica: RAND Corporation, P-3544, 1967).

أدى هذا إلى تقرير العام 1970 الذي أعده فريق عمل مجلس علوم الدفاع، المعروف باسم هيئة الحرب the Ware Panel ، Security Controls for Computer Systems (declassified by RAND Corporation as R-609-1, 1979)

ومقابلات.

(10) فهم وير جيدا وجهة النظر من أربانت:

Willis H. Ware, RAND and the Information Evolution: A History in Essays and Vignettes (Santa Monica: RAND Corporation, 2008).

(11) كان وير مهتما بهذه المشكلة على نحو خاص: المصدر نفسه، ص 155 وما يليها.

(12) في العام 1980، كان لورانس لاسكر Lawrence Lasker ووالتر باركز Walter Parkes:

Extra features, WarGames: The 25th Anniversary Edition, Blu-ray disc;

ومقابلات.

(13) كانت جذور وكالة الأمن القومي: انظر Kahn, The Codebreakers, 352.

الروايات عن الطابق العاشر من السفارة ورد فعل إنمان تجاه بلاغات الحريق، مصدرها من مقابلات. حقيقة أن الاستخبارات الأمريكية كانت تستمع إلى محادثات «بريجنيف» الخاصة في الليموزين (على الرغم من أنه لم يكن أسلوبها) كُشف عنها بواسطة: Jack Anderson, CIA Eavesdrops on Kremlin Chiefs," Washington Post, Sept. 16, 1971.

كان مصدر أندرسون معاونا يمينيا في مجلس الشيوخ، دفع بأن السجلات أثبتت أن الروس خانوا معاهدة الحد من الأسلحة النووية الأخيرة. بعد ظهور رواية أندرسون، بدأ الروس بتشفير اتصالاتهم الهاتفية، وكسرت وكالة الأمن القومي رموز الشفرة. ثم نصب الروس تشفيرا أكثر تطورا، وكان ذلك نهاية العملية. (مصدر كل هذه الخلفية هو مقابلات).

(14) في فترته الرئاسية الثانية:

Don Oberdorfer, From the Cold War to a New Era (Baltimore: Johns Hopkins University Press, 1998), 67.

(15) حينما اكتشفوا أمر الموجات الميكروية (ميكروويف):

Associated Press, "Russia Admits Microwaves Shot at US Embassy," July 26, 1976; "Science: Moscow Microwaves," Time, Feb. 23, 1976.

وتشير التقارير الإخبارية إلى أن موظفي الطابق العاشر كانوا يعانون مشكلات صحية بسبب أشعة الموجات الميكروية (ميكروويف). لم تكشف الروايات - ربما لم يعرف الصحافيون - الغرض من الأشعة أو الأنشطة في الطابق العاشر (يقتبسون أن مسؤولي السفارة يقولون إنهم في حيرة من أمرها).

(16) يداومون على تشغيل موسيقى خفيفة من نوعية «ميوزاك» Muzak في مكاتبهم في أثناء العمل: بصفتي مراسلا للدفاع في صحيفة «بوسطن غلوب» The Boston Globe في الثمانينيات من القرن العشرين، فحينما قابلت كبار مسؤولي البنتاغون في مكاتبهم، كنت في كثير من الأحيان أسمع موسيقى خفيفة من نوعية «ميوزاك» Muzak، وسألت أحدهم: لماذا كان يشغلها، فأشار إلى نافذته التي كانت تطل على نهر «بوتوماك» Potomac، وقال إنه ربما كان الروس يستمعون بأشعة الموجات الميكروية (ميكروويف).

الفصل الثاني

(1) كانت مهمته الأولى: معظم هذا مصدره من مقابلات، لكن انظر أيضا:

Christopher Ford and David Rosenberg, The Admirals' Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War (Annapolis: Naval Institute Press, 2005), esp. Ch. 5.

(جميع المواد بشأن «عاصفة الصحراء» مصدرها من مقابلات)

(2) اعتدل ماكونيل في جلسته حينما شاهد: على الرغم من أن فيلم «المتسللون» Sneakers كان مصدر إلهام لماكونيل ليطلق على هذا المفهوم «وسائل حرب المعلومات»، فإن هذه العبارة كانت قد استخدمت من قبل؛ أولا استخدمها عالم الأسلحة «توماس بي رونا» Thomas P. Rona في دراسة إفرادية monograph لشركة «بوينغ»

Boeing ", "Weapon Systems and Information War" (Boeing Aerospace Company, July 1976).

لم يكن رونا يشير إلى الحواسيب بل إلى التكنولوجيا التي عززت نظريا قدرة أنظمة أسلحة معينة من خلال ربطها بأجهزة استشعار (مستشعرات) استخباراتية.

(3) «فصل رأس هيكل قيادة العدو عن جسده من القوات المقاتلة»: Warner, "Cybersecurity: A Pre-history."

(4) جاهد ماكونيل بقوة من أجل «رقاقة كليبر»:

Jeffrey R. Yost, "An Interview with Dorothy E. Denning," OH 424, Computer Security History Project, April 11, 2013, Charles Babbage Institute, University of Minnesota, http://conservancy.umn.edu/bitstream/handle/11299/156519/oh424ded.pdf?sequence=1;

ومقابلات.

الفصل الثالث

(1) «البنية الأساسية القومية الحرجة البالغة الأهمية»:

President Bill Clinton, PDD-39, “U.S. Policy on Counterterrorism,” June 21, 1995, http://fas.org/irp/offdocs/pdd/pdd-39.pdf.

(2) حولت رينو المهمة: معظم المواد عن مجموعة عمل البنية الأساسية الحرجة مصدرها مقابلات مع مشاركين عدة، على الرغم من أن بعضها من:

Kathi Ann Brown, Critical Path: A Brief History of Critical Infrastructure Protection in the United States (Fairfax, VA: Spectrum Publishing Group, 2006), Chs. 5, 6.

كل التفاصيل حول جلسات الإحاطة والمحادثات الخاصة داخل المجموعة مصدرها من مقابلات.

(3) «مسائل التكنولوجيا الفائقة»: مذكرة، جوان هاريس JoAnn Harris، من خلال نائب المدعي العام جايمي جوريليك Jamie Gorelick، إلى المدعي العام.

Computer Crime Initiative Action Plan,” May 6, 1994; Memo, Deputy Attorney General [Gorelick], “Formation of Information Infrastructure Task Force Coordinating Committee,” July 19, 1994 (provided to author)

ومقابلات.

(4) في آونة أخيرة:

Hearings Before the Permanent Subcommittee on Investigations of the Comm. on Government Affairs. 104th Cong. (1996).

(بيان جايمي جوريليك Jamie Gorelick، نائب المدعي العام في الولايات المتحدة).

(5) والاجتماعات المشتركة بين الوكالات مع ستوديمان: دور ستوديمان في هيئات مشتركة بين الوكالات مصدرها من

Douglas F. Garthoff, Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946–2005 (Washington, D.C.: CIA Center for the Study of Intelligence, 2005), 267.

الإشارة إلى أنه كان يجتمع مع جوريليك كل أسبوعين ذكرت في:

Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations of the Comm. on Government Affairs. 104th Cong. (1996)

(بيان جايمي جوريليك Jamie Gorelick، نائب المدعي العام في الولايات المتحدة).

(6) كان أحد فروع «القسم جيه»: نظرية «العقد الحرجة» Critical nodes لم تفلح في الحروب الحقيقية. ركزت خطة هجوم سلاح الجو في حرب الخليج 1990-1991 على أربعة وثمانين هدفا باعتبارها «العقد» الرئيسية: دمر تلك الأهداف، وسينهار النظام وكأنه بيت من أوراق اللعب. في الواقع، لم تنته الحرب حتى سحق نصف مليون جندي من القوات الأمريكية وقوات التحالف الجيش العراقي على الأرض. انظر:

Michael Gordon and Bernard Trainor, The Generals’ War (New York: Little, Brown, 1995), Ch. 4; Fred Kaplan, Daydream Believers (Hoboken: John Wiley & Sons, 2008), 20–21.

(7) تتويجا للبيان الذي قدمه جرين: Brown, Critical Path, 78; and i ومقابلات

(8) «في ضوء اتساع: هذه الصياغة اللغوية استنسخت في مذكرة من المدعي العام إلى مجلس الأمن القومي، في 16 مارس، http://fas.org/sgp/othergov/munromem.htm

(9) كلمة واحدة كانت تحوم: أول استخدام لـ «الحرب السيبرانية» كان على الأرجح هو:
John Arquilla and David Ronfeldt, Cyberwar Is Coming! (Santa Monica: RAND Corporation, 1993),
لكن استخدامهم لهذه العبارة كان أشبه بما أطلق عليه «وسائل الحرب العاصفة» netcentric warfare أو «الثورة في الشؤون العسكرية»، وليس «الحرب السيبرانية» بالمفهوم الذي صارت عليه لاحقا.

(10) ربما شهدت ما يصل إلى 250,000 اعتداء:
General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks" (GAO/AIMD-96-84), May 22, 1996.
يعزى التقدير إلى دراسة أجرتها وكالة أمن معلومات الدفاع في البنتاغون.

(11) «بعض البنى الأساسية القومية:
President Bill Clinton, Executive Order 13010, "Critical Infrastructure Protection," July 15, 1996, http://fas.org/irp/offdocs/eo13010.htm.

(12) «ليس لدينا بعد هجوم سيبراني إرهابي:
Jamie Gorelick, Security in Cyberspace: Hearings Before the Permanent Subcommittee on Investigations of the Comm. on Government Affairs. 104th Cong. (1996)
(بيان «جايمي جوريليك» Jamie Gorelick، نائب المدعي العام في الولايات المتحدة).

(13) كانت برامج أمريكا في هذا المجال: لم يكن هناك سوى بضع زلات في الكشف عن وجود برنامج هجوم سيبراني، ولم يلاحظها سوى عدد قليل. في مايو من العام 1995، فإن إيميت بايج Emmett Paige، مساعد وزير الدفاع لشؤون القيادة والسيطرة والاتصالات والاستخبارات، قال في مؤتمر عقد في جامعة الدفاع القومي، «لدينا قدرة هجومية [سيبرانية]، لكننا لا نستطيع مناقشتها.... ستشعر بالرضا عنها إذا عرفتها». في الشهر التالي، قال الكابتن البحري (العقيد البحري) وليام جرافيل William Gravell، مدير مجموعة وسائل حرب المعلومات في هيئة الأركان المشتركة، في مؤتمر بأرلينجتون Arlington، «نحن في المرحلة الأولى من جهد شامل [في وسائل حرب المعلومات].... ما نقوم به حتى الآن هو بناء بعض الأنظمة الهجومية القوية جدا». وأضاف: «حتى الآن لا توجد سياسة حالية في هذه الأمور». وسيبقى ذلك صحيحا لسنوات كثيرة مقبلة. هذان التصريحان اقتبسا في:
Neil Munro, "Pentagon Developing Cyberspace Weapons," Washington Technology, June 22, 1995—with no follow-up in any mass media, http://washingtontechnology.com/Articles/1995/06/22/Pentagon-Developing-Cyberspace-Weapons.aspx.

(14) عقد مارش وأعضاء اللجنة اجتماعهم الأول في: Brown, Critical Path, 93. باقي المواد عن اللجنة مصدرها من مقابلات.

(15) ودعتنا الأسلحة الرهيبة بعيدة المدى

White House, Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection, Oct. 1997, http://fas.org/sgp/library/pccip.pdf.

(16) تهديد جاد خطير للبنية الأساسية للاتصالات:

Commission on Engineering and Technical Systems, National Research Council, Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness(Washington, D.C.: National Academy Press, 1989), 9.

(17) اللص المعاصر:

Commission on Engineering and Technical Systems, National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington, D.C.: National Academy Press, 1991), 7.

(18) «الاعتماد المتزايد»:

Report of the Defense Science Board Task Force on Information Warfare-Defense (Washington, D.C.: Office of the Undersecretary of Defense [Acquisition and Technology], 1996).

الاقتباسات من: Duane Andrews, cover letter to Craig Fields, Nov. 27, 1996.

(19) «في جهودنا لمكافحة: نص خطاب الرئيس بيل كلينتون في الأكاديمية البحرية في أنابوليس، 22 مايو من العام 1998.

Transcript, President Bill Clinton, Address to Naval Academy, Annapolis, MD, May 22, 1998, http://www.cnn.com/ALLPOLITICS/1998/05/22/clinton.academy/transcript.html.

الفصل الرابع

(1) في 9 يونيو من العام 1997: معظم المواد عن تدريب «المتلقي المؤهل» مصدرها مقابلات مع مشاركين، لكن بعضها يأتي أيضا من هذه المصادر المطبوعة:

Brig. Gen. Bruce Wright, "Eligible Receiver 97," PowerPoint briefing, n.d. (declassified; obtained from the Cyber Conflict Studies Association); Dillon Zhou, "Findings on Past US Cyber Exercises for 'Cyber Exercises: Yesterday, Today and Tomorrow'" (Washington, D.C.: Cyber Conflict Studies Association, March 2012); Warner, "Cybersecurity: A Pre-history."

(2) حدثت أول حالة مرعبة كالكابوس: للمزيد عن «دودة (دودة حاسوبية) موريس» Morris Worm، انظر:

Cliff Stoll, The Cuckoo's Egg (New York: Doubleday, 1989), 385ff; Mark W. Eichin and Jon A. Rochlis, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988" (MIT, Feb. 9, 1989), presented at the 1989 IEEE Symposium on Research in Security and Privacy,

http://www.utdallas.edu/~edsha/UGsecurity/internet-worm-MIT.pdf.

(3) كان ابتكار تود هيبيرلين:

Richard Bejtlich, The Practice of Network Security Monitoring (San Francisco: No Starch Press, 2013), esp. the foreword (by Todd Heberlein) and Ch. 1; Richard Bejtlich, TAO Security blog, "Network Security Monitoring History," April 11, 2007, http://taosecurity.blogspot.com/2007/04/network-security-monitoring-history.html

; ومقابلات.

في وقت لاحق، صار بيجليك - الذي كان ضابطا في مركز سلاح الجو لوسائل حرب المعلومات - كبير ضباط الأمن في شركة «مانديانت»، إحدى الشركات الخاصة الرائدة في مجال الأمن السيبراني. ارتقى الرئيس المؤسس كيفن مانديا Kevin Mandia في صفوف سلاح الجو باعتباره اختصاصيا في الجريمة السيبرانية في مكتب التحقيقات الخاصة. وفي أثناء تلك الفترة، كان على نحو متكرر يزور مركز سلاح الجو لوسائل حرب المعلومات، حيث تعلم نظام رصد أمن الشبكات الذي كان لدى المركز الذي تأثر به على نحو كبير.

(4) كان أحد صغار الضباط: كان هذا هو بيجليك، انظر أحد إصدارات مراجعاته:

http://www.amazon.com/review/RLLSEQRTT5DIF

(5) «لافتة تحذيرية»:

Letter, Robert S. Mueller III, Assistant Attorney General, Criminal Division, to James H. Burrows, Director, Computer Systems Laboratory, National Institute of Standards and Technology, Department of Commerce, Oct. 7, 1992, http://www.netsq.com/Documents_html/DOJ_1992_letter/.

(6) حينما غادر مينيهان البنتاغون: Bejtlich, "Network Security Monitoring History."

(7) كان يتعين أن ترقى تلك الأنظمة إلى مستوى مرتفع: في الثمانينيات من القرن العشرين، كتب مركز أمن الحاسوب بمديرية ضمان المعلومات سلسلة من الكتيبات الإرشادية، وضع معايير «أنظمة الحاسوب الموثوق بها trusted computer systems». كانت الكتيبات الإرشادية تسمى «سلسلة قوس قزح» Rainbow Series نظرا إلى ألوان أغلفتها الزاهية. كان الكتاب الرئيسي هو الكتاب الأول، وهو الذي كان يطلق عليه «الكتاب البرتقالي»، «معايير تقييم أنظمة الحاسوب الموثوق بها» Trusted Computer Systems Evaluation Criteria، الذي نُشر في العام 1983. وقد أنجز معظم العمل مدير المركز، روجر شل Roger Schell، الذي كان قبل عقد من الزمن قد ساعد أجهزة الاستخبارات على النفاذ إلى أنظمة اتصالات الخصوم، ومن ثم عرف أن أنظمة الولايات المتحدة ستكون هي أيضا ضعيفة جدا وعرضة للهجوم.

(8) في 16 فبراير من العام 1997:

CJCS Instruction No. 3510.01, "No-Notice Interoperability Exercise (NIEX) Program," quoted in Zhou, "Findings on Past US Cyber Exercises for 'Cyber Exercises: Yesterday, Today and Tomorrow.'"

(9) حدد التدريب سيناريو يتكون من ثلاث مراحل: Wright, "Eligible Receiver 97," PowerPoint briefing. ويستند الجزء المتبقي من القسم إلى مقابلات مع مشاركين.

(10) لم يتردد الشخص الذي أجاب عن الهاتف: مات ديفوست من «فريق تقييم مواطن الضعف والثغرات الأمنية- التحالف» كان قد تعرض لمشكلات مماثلة حينما كان يحاول العثور على كلمة مرور الحاسوب الخاص بالقائد الأمريكي في أثناء إحدى المناورات الحربية للدول الخمس. أولا، أطلق العنان لبرمجية متوافرة على نطاق واسع، في غضون ثانية واحدة تقريبا، جربت كل كلمة في القاموس مع تنويعاتها. ثم اتصل هاتفيا بمكتب القائد، وقال إنه كان مع مجموعة رغبت منه أن يأتي للتحدث معه، وطلب ملخصا عن السيرة الذاتية. استخدم المعلومات الموجودة في تلك الورقة لتوليد كلمات مرور جديدة، واقتحم باستخدام كلمة «Rutgers» (حيث كان ابن القائد ذاهبا إلى الكلية) متبوعا بعدد مكون من رقمين.

(11) لم يقدم سوى لمحة موجزة:

White House, Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection, Oct. 1997, 8, http://fas.org/irp/offdocs/nsdd145.htm.

الفصل الخامس

(1) في 3 فبراير من العام 1998: قصة «الشروق الشمسي» مصدرها أساسا من مقابلات ولكن أيضا من

Richard Power, "Joy Riders: Mischief That Leads to Mayhem," InforMIT, Oct. 30, 2000, http://www.informit.com/articles/article.aspx?p=19603&seqNum=4; Solar Sunrise: Dawn of a New Threat, FBI training video, www.wired.com/2008/09/video-solar-sun/; Michael Warner, "Cybersecurity: A Pre-history;"

والمصادر المذكورة أدناه.

(2) «أولى طلقات: Bradley Graham, "US Studies a New Threat: Cyber Attack," Washington Post, May 24, 1998.

(3) «قلق من أن التسلل:

FBI, Memo, NID/CID to all field agents, Feb. 9, 1998 (declassified, obtained from the Cyber Conflict Studies Association).

(4) «مقدم على التقاعد: Power, "Joy Riders."

(5) «الهجوم الممنهج الأكثر تنظيما»:

Rajiv Chandrasekaran and Elizabeth Corcoran, "Teens Suspected of Breaking into U.S. Computers," Washington Post, Feb. 28, 1998.

(6) أما تنينباوم، فقد ألقت الشرطة الإسرائيلية القبض عليه:

Dan Reed and David L. Wilson, "Whiz-Kid Hacker Caught," San Jose Mercury News, March 19, 1998, http://web.archive.org/web/20001007150311/http://www.mercurycenter.com/archives/reprints/hacker110698.htm; Ofri Ilany, "Israeli Hacker Said Behind Global Ring That Stole Millions," Haaretz, Oct. 6, 2008, http://www.haaretz.com/print-edition/news/israeli-hacker-said-behind-global-ring-that-stole-millions-1.255053.

(7) «لا يزيد على كونه أحد الاختراقات المعتادة:
FBI, Memo, [sender and recipient redacted], "Multiple Intrusions at DoD Facilities," Feb. 12, 1998 (obtained from the Cyber Conflict Studies Association files).

(8) «من الذي يتولى زمام الأمور؟»:
Lessons from Our Cyber Past—The First Military Cyber Units," symposium transcript, Atlantic Council, March 5, 2012, http://www.atlanticcouncil.org/news/transcripts/transcript-lessons-from-our-cyber-past-the-first-military-cyber-units.

(9) «مسؤولة عن تنسيق:
Maj. Gen. John H. Campbell, PowerPoint presentation, United States Attorneys' National Conference, June 21, 2000.

(10) في تلك الأثناء، كان مكتب التحقيقات الفدرالي يتقصى جميع الأدلة: انظر الكثير من مذكرات مكتب التحقيقات الفدرالي، من المكاتب الميدانية المختلفة وإليها، في وثائق رفع عنها الحظر وحُصل عليها من «رابطة دراسات الصراع السيبراني Cyber Conflict Studies Association».

(11) 5.5 غيغابايت من البيانات: الرقم 5.5 غيغابايت مصدره:
Maj. Gen. John H. Campbell, PowerPoint briefing on computer network defense, United States Attorneys' National Conference, June 21, 2000.

(12) بعد أيام، تسربت الأخبار إلى الصحافة:
"Cyber War Underway on Pentagon Computers—Major Attack Through Russia," CNN, March 5, 1999; Barbara Starr, "Pentagon Cyber-War Attack Mounted Through Russia," ABC News, March 5, 1999, http://www.rense.com/politics2/cyberwar.htm.

(13) «طار الوفد إلى موسكو في 2 أبريل: ذكرت الرحلة في مذكرات مكتب التحقيقات الفدرالي التي رفع عنها الحظر، في ملفات «رابطة دراسات الصراع السيبراني» Cyber Conflict Studies Association: على سبيل المثال
FBI, Memo, from NatSec, "Moonlight Maze," March 31, 1999; FBI, Memo (names redacted), Secret/NoForn, "Moonlight Maze Coordinating Group," April 15, 1999.
بقية المواد مصدرها من مقابلات. (مذكرة 15 أبريل تذكر أيضا أن مسؤولي وزارة العدل ووزارة الدفاع، بمن في ذلك مايكل فاتيس Michael Vatis وسوب كامبل Soup Campbell، أطلعا الأعضاء الرئيسيين في لجان الاستخبارات في مجلس النواب ومجلس الشيوخ في 21 فبراير من العام 1999، وأن أول ذكر علني لـعملية «متاهة ضوء القمر» Moonlight Maze كان بواسطة جون هامري John Hamre في 5 مارس من العام 1999، بعد عام واحد من التسللات الأولى.

الفصل السادس

(1) علم كلارك أن تجمعهم قد بدأ: القسم الخاص بـ «مادج» ولوفت L0pht مصدره بشكل رئيسي من مقابلات، ولكن أيضا من:

Bruce Gottlieb, "HacK, CouNterHaCk," New York Times, Oct. 3, 1999; Michael Fitzgerald, "L0pht in Transition," CSO, April 17, 2007, http://www.csoonline.com/article/2121870/network-security/lopht-in-transition.html; "Legacy of the L0pht," IT Security Guru, http://itsecurityguru.org/gurus/legacy-l0pht/#.VGE-CIvF_QU.

في وقت لاحق كتب كلارك Clarke رواية:

Breakpoint (New York: G. P. Putnam's Sons, 2007(

التي كانت إحدى الشخصيات الرئيسية، سوكستر Soxster، مستوحاة من مادج Mudge؛ ومخترق سري تحت الأرض يسمى «المخبأ» The Dugout على غرار لوفت L0pht.

(2) كان زاتكو قرصان حاسوب (هاكر): عزفه على الجيتار في «بيركلي» مصدره

Mark Small, "Other Paths: Some High-Achieving Alumni Have Chosen Career Paths That Have Led Them to Surprising Places," Berklee, Fall 2007, .http://www.berklee.edu/bt/192/other_paths.html

(3) أول ظهور له وأعضاء لوفت الآخرون: يمكن مشاهدة جلسة الاستماع على «يوتيوب»:

http://www.youtube.com/watch?v=VVJldn_MmMY

(4) بعد ثلاثة أيام من إدلاء مادج بشهادته:

Bill Clinton, Presidential Decision Directive/NSC-63, "Critical Infrastructure Protection," May 22, 1998, http://fas.org/irp/offdocs/pdd/pdd-63.htm.

(5) شبكة فدرالية لكشف التسلل أطلق عليها اسم «فيدنت» FIDNET:

John Markoff, "U.S. Drawing Plan That Will Monitor Computer Systems," New York Times, July 28, 1999;

ومقابلات.

(6) «أورويلية» Orwellian:

Tim Weiner, "Author of Computer Surveillance Plan Tries to Ease Fears," New York Times, Aug. 16, 1999;

ومقابلات.

(7) «في حين يستطيع الرئيس والكونجرس إصدار أمر:

Bill Clinton, National Plan for Information Systems Protection, Jan. 7, 2000, http://cryptome.org/cybersec-plan.htm.

(8) مع ذلك، أقنع كلارك الرئيس بعقد قمة: معظم هذا مصدره من مقابلات، ولكن انظر أيضا:

Gene Spafford, "Infosecurity Summit at the White House," Feb. 2000, http://spaf.cerias.purdue.edu/usgov/pres.html; CNN, Morning News, Feb. 15, 2000, http://transcripts.cnn.com/TRANSCRIPTS/0002/15/mn.10.html; Ricardo Alonso-Zaldivar and Eric Lichtblau, "High-Tech Industry Plans to Unite Against Hackers," Los Angeles Times, Feb. 16, 2000.

(9) قبل ذلك ببضعة أسابيع، كان مادج قد أصبح قانونيا:

Kevin Ferguson, "A Short, Strange Trip from Hackers to Entrepreneurs," Businessweek Online Frontier, March 2, 2000, http://www.businessweek.com/smallbiz/0003/ep000302.htm?scriptframed.

الفصل السابع

(1) «الأول من نوعه:

U.S. Air Force, 609 IWS: A Brief History, Oct 1995–Jun 1999, https://securitycritics.org/wp-content/uploads/2006/03/hist-609.pdf.

(2) «أي إجراء من شأنه أن يحجب، أو يستغل:

U.S. Air Force, Cornerstones of Information Warfare, April 4, 1997, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA323807/.

(3) خاضت الوحدة «جيه - 39» أولى مغامراتها الحربية: حول عملية «تانجو» Tango (وإن لم يكن دور جيه - 39)، انظر:

Richard H. Curtiss, "As U.S. Shifts in Bosnia, NATO Gets Serious About War Criminals," Christian Science Monitor, July 18, 1997؛ ومقابلات.

(4) أكثر من ثلاثين ألف جندي من قوات حلف شمال الأطلسي (الناتو):

NATO, "History of the NATO-led Stabilisation Force (SFOR) in Bosnia and Herzegovina," http://www.nato.int/sfor/docu/d981116a.htm.

(5) «في آن واحد نجاح كبير:

Admiral James O. Ellis, "A View from the Top," PowerPoint presentation, n.d., http://www.slideserve.com/nili/a-view-from-the-top-admiral-james-o-ellis-u-s-navy-commander-in-chief-u-s-naval-forces-europe-commander-allied.

الفصل الثامن

(1) في صيف العام 1998: حاول سلاح الجو امتلاك زمام «فريق العمل المشترك لحماية شبكات الحاسوب» (جيه تي إف - سي إن دي) ، بذريعة أن مركز وسائل حرب المعلومات كان لديه موارد وخبرات فريدة من نوعها لهذه المهمة، لكن آرت موني Art Money وجون هامري John Hamre كانا يعتقدان بضرورة أن تكون مؤسسة إما تشمل جميع الفروع وإما تفوقها. ومقابلات.

(2) لذلك، في 1 أبريل من العام 2000:

U.S. Space Command, "JTF-GNO History—The Early Years of Cyber Defense," Sept. 2010; and interviews.

ومقابلات.

(3) وبوصفه منهجي التفكير يهوى:

GEDA is cited by Richard Bejtlich, "Thoughts on Military Service," TAO Security blog, Aug. 3, 2006, http://taosecurity.blogspot.com/2006/08/thoughts-on-military-service.html

ومقابلات.

(4) على نحو مفاجئ، ومن دون سابق إنذار، وإن لم يكن ذلك إلا من أجل دعم مطالبهم:
William M. Arkin, “A Mouse That Roars?,” Washington Post, June 7, 1999; Andrew Marshall, “CIA Plan to Topple Milosevic ‘Absurd,’ ” The Independent, July 8, 1999

ومقابلات.

(5) ومن أجل الحفاظ على وكالة الأمن القومي في مركز هذا العالم:
NSA/CSS, Transition 2001, Dec. 2000, http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf; George Tenet, CIA Director, testimony, Senate Select Committee on Government Affairs, June 24, 1998, https://www.cia.gov/news-information/speeches-testimony/1998/dci_testimony_062498.html; Arkin, “A Mouse That Roars?”;

ومقابلات.

(6) كتب التقرير المجموعة الاستشارية التقنية: معظم قسم المجموعة الاستشارية التقنية مصدره من المقابلات، ذُكر تقرير المجموعة الاستشارية التقنية في:
Douglas F. Garthoff, Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946–2005 (Washington, D.C.: CIA Center for the Study of Intelligence, 2005), 273.

(7) أخذت لجنة مجلس الشيوخ تقريره بجدية بالغة:
Senate Select Committee on Intelligence, Authorizing Appropriations for Fiscal Year 2001 for the Intelligence Activities of the United States Government, Senate Rept. 106-279, 106th Congress, May 4, 2000, https://www.congress.gov/congressional-report/106th-congress/senate-report/279/1

; ومقابلات.

(8) «رداءة في تعريف مهمتها»:
NSA/CSS, External Team Report: A Management Review for the Director, NSA, Oct. 22, 1999, http://fas.org/irp/nsa/106handbk.pdf

; ومقابلات.

(9) «منظمة غير متسقة»:
NSA/CSS, “New Enterprise Team (NETeam) Recommendations: The Director’s Work Plan for Change,” Oct. 1, 1999, http://cryptome.org/nsa-reorg-net.htm.

(10) في 15 نوفمبر، دشن:
Seymour M. Hersh, “The Intelligence Gap,” The New Yorker, Dec. 6, 1999

; ومقابلات.

(11) تعطل نظام الحاسوب الرئيسي في وكالة الأمن القومي:
US Intelligence Computer Crashes for Nearly 3 Days,” CNN.com, Jan. 29, 2000, http://edition.cnn.com/2000/US/01/29/nsa.computer/;

ومقابلات.

(12) أطلق هايدن على البرنامج الجديد اسم «الرائد» Trailblazer:

NSA Press Release, "National Security Agency Awards Concept Studies for Trailblazer," April 2, 2001, https://www.nsa.gov/public_info/press_room/2001/trailblazer.shtml; Alice Lipowicz, "Trailblazer Loses Its Way," Washington Technology, Sept. 10, 2005, https://washingtontechnology.com/articles/2005/09/10/trailblazer-loses-its-way.aspx

(13) كانت مؤسسة «ساينس أبليكشانز إنترناشيونال» (المؤسسة الدولية للتطبيقات العلمية) بوجه خاص متداخلة جدا:

Siobhan Gorman, "Little-Known Contractor Has Close Ties with Staff of NSA," Baltimore Sun, Jan. 29, 2006, http://articles.baltimoresun.com/2006-01-29/news/0601290158_1_saic-information-technology-intelligence-experts; "Search Top Secret America's Database of Private Spooks," Wired, July 19, 2010, http://www.wired.com/2010/07/search-through-top-secret-americas-network-of-private-spooks/.

(14) في الأعوام التالية، كانت صفوف «مكتب عمليات الولوج المصمم وفقا للحاجة» (تاو - تي إيه أوو) ستزداد وتتضخم:

"Inside TAO: Documents Reveal Top NSA Hacking Unit," Der Spiegel, Dec. 29, 2013, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

(15) كانت طرائق تشغيل ووجود تلك الأجهزة:

Matthew M. Aid, "Inside the NSA's Ultra-Secret China Hacking Group," Foreign Policy, June 10, 2013.

(16) أحد الأجهزة، يسمى «لاود أوتو» LoudAuto: مصدر أسماء هذه البرامج من كتالوج «مكتب عمليات الولوج المُصَمَّم وفقا للحاجة» (تاو - تي إيه أوو) المكون من 58 صفحة من الأدوات والتقنيات، من بين الكثير من الوثائق التي تسربت بواسطة إدوارد سنودِن Edward Snowden المقاول السابق لوكالة الأمن القومي. لم تطبع أي صحيفة أو مجلة في الولايات المتحدة القائمة (كان الصحافيون والمحررون الذين كانوا يعملون على القصة اعتبروها ضارة بشكل حقيقي للأمن القومي)، لكن صحيفة «دير شبيغل» Der Spiegel، نشرتها

(Jacob Appelbaum, Judith Horchert, and Christian Stöcker, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox," Dec. 29, 2013)

وبعد ذلك أعاد بروس شناير Bruce Schneier، محلل أمن الحاسوب، طباعة كل عنصر على مدونته.

(17) كلما كان قراصنة الحاسوب (الهاكرز) والجواسيس يكتشفون أوجه الضعف والثغرات الأمنية: «داخل مكتب عمليات الولوج المُصَمَّم وفقا للحاجة» (Office of Tailored Access Operations (TAO.

(18) في العقد اللاحق، انطلقت شركات خاصة: للمزيد حول الثغرات الأمنية التي لم يكن أحد قد اكتشفها بعد والتي يمكن استغلالها بشكل فوري من دون انتظار (zero-day exploits): انظر:

Neal Ungerleider, "How Spies, Hackers, and the Government Bolster a Booming Software Exploit Market," Fast Company, May 1, 2013; Nicole

Perlroth and David E. Sanger, “Nations Buying as Hackers Sell Flaws in Computer Code,” New York Times, July 13, 2013; Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon (New York: Crown, 2014).

روايات محددة مصدرها من مُقابلات.

(19) في أثناء الأشهر القليلة الأولى من فترة ولاية بوش:

Richard A. Clarke, Against All Enemies (New York: Free Press, 2004); Steve Coll, Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001 (New York: Penguin, 2004), 435.

(20) في يوم هجمات الحادي عشر من سبتمبر:

Robin Wright, “Top Focus Before 9/11 Wasn’t on Terrorism,” Washington Post, April 1, 2004.

(21) دعته رايس إلى إعداد مُسَوَّدة لأمر تنفيذي يدعو إلى خطة جديدة:

Executive Order 13226—President’s Council of Advisors on Science and Technology, Sept. 30, 2001, http://www.gpo.gov/fdsys/pkg/WCPD-2001-10-08/pdf/WCPD-2001-10-08-Pg1399.pdf

الخلفية، وقاعات المدينة، وما إلى ذلك مصدرها من مُقابلات.

(22) وكما تبين، فإن المُسَوَّدة النهائية:

President George W. Bush, The National Strategy to Secure Cyberspace, Feb. 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

الفصل التاسع

(1) حينما تولى الجنرال جون أبي زَيد John Abizaid: للمزيد عن أبي زيد وحرب العراق، انظر:

Fred Kaplan, The Insurgents: David Petraeus and the Plot to Change the American Way of War (New York: Simon & Schuster, 2013), esp. 182;

بقية هذا القسم مصدرها من مُقابلات.

(2) في الوقت نفسه، فإن وزير الدفاع دونالد رامسفيلد Donald Rumsfeld: انظر المصدر نفسه، الفصل الرابع.

(3) كانت سبعة عشر عاما قد مرت:

https://www.nsa.gov/about/leadership/former_directors.shtm.

(4) في ذات الشهر، وقَّع رامسفيلد:

Dana Priest and William Arkin, Top Secret America: The Rise of the New American Security State (New York: Little, Brown, 2011), 236.

(5) قبل ذلك ببضعة أعوام، حينما كان ألكسندر: المقطع عن عداء ألكسندر هايدن Alexander-Hayden وتجربة جيمس هيث James Heath في «فورت بيلفوار» مصدره من مُقابلات. بعض المواد عن هيث مصدرها أيضا من:

Shane Harris, “The Cowboy of the NSA,” Foreign Policy, Sept. 2013; and

Shane Harris, The Watchers: The Rise of America's Surveillance State (New York: Penguin, 2010), 99, 135.

ذكر البعض أن ألكسندر صمم منصب قائد «مركز الهيمنة المعلوماتية» ليبدو مثل القبطان على «ستار تريك» Star Trek، لكن في الواقع، لم يؤسس بواسطة ألكسندر، أو حتى بواسطة نونان Noonan، بل بالأحرى بواسطة سلف نونان، الميجور جنرال جون توماس.

Ryan Gallagher, "Inside the U.S. Army's Secretive Star Trek Surveillance Lair," Slate, Sept. 18, 2013, http://www.slate.com/blogs/future_tense/2013/09/18/surveilliance_and_spying_does_the_army_have_a_star_trek_lair.html;

ومُقابلات.

(6) لكن ألكسندر نال ثقة رامسفيلد: معظم هذا مصدره من مُقابلات، لكن نقل البيانات في يونيو من العام 2001 ذكر أيضا في:

Keith Alexander, classified testimony before House Permanent Select Committee on Intelligence, Nov. 14, 2001, reprinted in U.S. Army Intelligence and Security Command, Annual Command History, Fiscal Year 2001, Sept. 30, 2002

(رفع عنه الحظر بموجب قانون حرية المعلومات).

(7) من المفارقات التي تدعو إلى السخرية، أنه في حين أن هايدن كان يشكو: للحصول على تفاصيل حول «رياح ستيلار» Stellar Wind، انظر:

Barton Gellman, "U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata," Washington Post, June 15, 2013, and, attached on the Post website, the top secret draft of an inspector general's report on the program, http://apps.washingtonpost.com/g/page/world/national-security-agency-inspector-general-draft-report/277/.

(8) كان المشروع «ترايلبلايزر» قد استهلك 1.2 مليار دولار:

Siobhan Gorman, "System Error," Baltimore Sun, Jan. 29, 2006, http://articles.baltimoresun.com/2006-01-29/news/0601280286_1_intelligence-experts-11-intelligence-trailblazer; Alice Lipowicz, "Trailblazer Loses Its Way," Washington Technology, Sept. 10, 2005, http://washingtontechnology.com/articles/2005/09/10/trailblazer-loses-its-way.aspx;

ومُقابلات.

(9) كان «تيربِلانس» (صخب) يتألف من تسعة نظم أصغر:

Robert Sesek, "Unraveling NSA's Turbulence Programs," Sept. 15, 2014, https://robert.sesek.com/2014/9/unraveling_nsa_s_turbulence_programs.html;

ومقابلات.

(10) بدأت «بوابة الوقت الحقيقي الإقليمية» (آر تي آر جي): مصدر هذا أساسا من مقابلات، ولكن أيضا من:

Bob Woodward, Obama's Wars (New York: Simon & Schuster, 2010), 10;

Ellen Nakashima and Joby Warrick, "For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All,'" Washington Post, July 14, 2013; Shane Harris, @War: The Rise of the Military-Internet Complex (New York: Houghton Mifflin Harcourt, 2014), Ch. 2.

(11) في العام 2007 وحده، فإن تلك النوعيات من العمليات:

"General Keith Alexander Reveals Cybersecurity Strategies and the Need to Secure the Infrastructure," Gartner Security and Risk Management Summit, June 23–26, 2014, http://blogs.gartner.com/security-summit/announcements/general-keith-alexander-reveals-cybersecurity-strategies-and-the-need-to-secure-the-infrastructure/;

ومقابلات.

(12) لم يكن التأثير حاسما ساحقا: للمزيد حول هذه النقطة، انظر: Kaplan, The Insurgents, esp. Ch. 19.

(13) في 6 سبتمبر:

David A. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis," Aviation Week & Space Technology, Nov. 12, 2013; Erich Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," Der Spiegel, Nov. 2, 2009, http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html; Richard A. Clarke and Robert A. Knake, Cyber War (New York: HarperCollins, 2010), 1–8; Robin Wright, "N. Koreans Taped at Syrian Reactor," Washington Post, April 24, 2008; "CIA Footage in Full," BBC News, April 24, 2008, http://news.bbc.co.uk/2/hi/7366235.stm;

ومقابلات.

(14) قامت الوحدة 8200 بذلك الاختراق باستخدام برنامج حاسوبي كان يسمى «سوتِر» Suter:

Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis";

ومقابلات.

كان هناك جدل حول ما إذا كان الهدف بالفعل مفاعلا نوويا، ولكن بالتأمل في الماضي، يبدو الدليل غير قابل للجدل. من بين أمور أخرى، وجدت الوكالة الدولية للطاقة الذرية، في عينات التربة التي جمعتها حول المفاعل الذي قُصف، «عددا كبيرا من جزيئات اليورانيوم الطبيعية البشرية المنشأ (أي، أُنتجت نتيجة المعالجة الكيميائية)».
(Follath and Stark, "The Story of 'Operation Orchard")

(15) قبل ذلك بأربعة أشهر ونصف الشهر:

"War in the Fifth Domain," The Economist, July 1, 2010, http://www.economist.com/node/16478792; Andreas Schmidt, "The Estonian Cyberattacks," in Jason Healey, ed., A Fierce Domain, 174–93; Clarke and Knake, Cyber War, 12–16.

(16) في 1 أغسطس من العام 2008، قام الانفصاليون في أوسيتيا:

U.S. Cyber Consequences Unit, Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008 (Aug. 2009), http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf; Andreas Hagen, "The Russo-Georgian War, 2008," in Healey, ed., A Fierce Domain, 194–204; Government of Georgia, Ministry of Foreign Affairs, Russian Invasion of Georgia: Russian Cyberwar on Georgia (Nov. 10, 2008), http://www.mfa.gov.ge/files/556_10535_798405_Annex87_CyberAttacks.pdf.

(17) للإجابة عن ذلك السؤال، أجرت وزارة الطاقة في 4 مارس من العام 2007 تجربة أُطلق عليها اسم «اختبار المولِد الكهربائي أورورا» Aurora Generator Test: خلفية الاختبار مصدرها من مقابلات. انظر أيضا:

"Mouse Click Could Plunge City into Darkness, Experts Say," CNN, Sept. 27, 2007, http://www.cnn.com/2007/US/09/27/power.at.risk/index.html; Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon (New York: Crown, 2014), Ch. 9.

(18) على نحو فوري تقريبا، اهتز الْمُولِّد: للفيديو، انظر

https://www.youtube.com/watch?v=fJyWngDco3g.

(19) في العام 2000، فإن موظفا ساخطا وناقما: Zetter, Countdown to Zero Day, 135ff..

الفصل العاشر

(1) حينما استُحدث المنصب: Fred Kaplan, "The Professional," New York Times Magazine, Feb. 10, 2008.

(2) لذا، فإن جلسة إحاطة ماكونيل: موعد الاجتماع مصدره من:

"NSC 05/16/2007-Cyber Terror" folder, NSC Meetings series, National Security Council-Records and Access Management Collection, George W. Bush Presidential Library

(مجلد حُصل عليه من خلال قانون حرية المعلومات). مضمون الاجتماع (الذي لم تُرفع السرية عنه) مصدره من مقابلات.

(3) التقط بوش الفكرة سريعا: هذا اعتمادا على مقابلات، على الرغم من أنه مشمول أيضا في:

Shane Harris, @War: The Rise of the Military-Internet Complex (New York: Houghton Mifflin Harcourt, 2014), Ch. 2.

(4) لكن تبدى أن المهمة يتعذر تنفيذها:

William Jackson, "DHS Coming Up Short on Einstein Deployment," GCN, May 13, 2003, http://gcn.com/articles/2013/05/13/dhs-einstein-deployment.aspx;

ومقابلات.

(5) في 9 يناير من العام 2008:

President George W. Bush, National Security Presidential Directive

(NSPD) 54, "Cyber Security Policy," Jan. 8, 2008, http://www.fas.org/irp/offdocs/nspd/nspd-54.pdf.

الخلفية مصدرها من مقابلات.

(6) في أثناء ذلك، قامت وزارة الأمن الداخلي بتحديث آينشتاين:

Steven M. Bellovin et al., "Can It Really Work? Problems with Extending Einstein 3 to Critical Infrastructure," Harvard National Security Journal, Vol. 3, Jan. 2011, http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Bellovin_Bradner_Diffie_Landau_Rexford.pdf;

ومقابلات.

(7) كان ألكسندر يعمم وينشر المقولة:

Alexander cited the "Maginot Line" analogy many times; see for instance, "Defenses Against Hackers Are Like the 'Maginot Line,' NSA Chief Says," Blog, WSJ Tech, Jan. 13, 2012, http://blogs.wsj.com/digits/2012/01/13/u-s-business-defenses-against-hackers-are-like-the-maginot-line-nsa-chief-says/;;

ومقابلات.

(8) أتت اللحظة المحورية الحاسمة: الجزء الخاص بـعملية «اليانكي صائد الظباء» Buckshot Yankee بشكل رئيسي مصدرها من مُقابلات، ولكن أيضا من:

Karl Grindal, "Operation Buckshot Yankee," in Jason Healey, ed., A Fierce Domain: Conflict in Cyberspace 1986 to 2012 (Washington, D.C.: Atlantic Council, 2013); Harris, @War, Ch. 9; William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," Foreign Affairs, Sept./Oct. 2010.

(9) عند بداية توليه المنصب: للمزيد عن غيتس وزيرا للدفاع، انظر

Kaplan, "The Professional"; and Kaplan, The Insurgents: David Petraeus and the Plot to Change the American Way of War (New York: Simon & Schuster, 2013), Ch. 18.

(10) في 23 يونيو من العام 2009:

U.S. Dept. of Defense, "U.S. Cyber Command Fact Sheet," May 25, 2010, http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-038.pdf.

(11) في 7 يوليو من العام 2010، كان غيتس يتناول طعام الغداء: هذا القسم مصدره أساسا من مقابلات، على الرغم من الإشارة إلى الخطة باختصار، إلى جانب مواعيد الاجتماعين، في:

Robert Gates, Duty: Memoirs of a Secretary at War (New York: Alfred A. Knopf, 2014), 450–51.

(12) «ساحة حرب»: يستند هذا القسم بشكل رئيسي إلى مُقابلات، على الرغم من أنه في ملف «رويترز»، عند استقالتها في العام 2013، قال لوت، «لقد تطورت السرود الوطنية حول السيبرانية. إنها ليست ساحة حرب، وبالتأكيد لا يمكننا التعامل معها كما لو كانت ساحة حرب. نحن لن نديرها كما لو أنها برنامج استخباراتي أو عملية كبيرة لإنفاذ القانون».

)Joseph Menn, "Exclusive: Homeland Security Deputy Director to Quit; Defended Civilian Internet Role," Reuters, April 9, 2013, http://www.reuters.com/article/2013/04/09/us-usa-homeland-lute-idUSBRE9380DL20130409.(

(13) في نهاية المطاف، وافقوا على أن يكون براون: النسخة المبسطة من الاتفاق، «مذكرة اتفاق بين وزارة الأمن الداخلي ووزارة الدفاع بشأن الأمن السيبراني»، التي وقعها غيتس في 24 سبتمبر ونابوليتانو في 27 سبتمبر من العام 2010، يمكن الاطلاع عليها في:
http://www.defense.gov/news/d20101013moa.pdf.

الفصل الحادي عشر

(1) أدت جلسات الاستماع إلى إصدار «قانون مُراقبة الاستخبارات الأجنبية: القسم الخاص بقانون مراقبة الاستخبارات الأجنبية الذي يتناول المراقبة الإلكترونية هو: 50 U.S.C. 1802(a).

(2) بعد هجمات الحادي عشر من سبتمبر: ملخص جيد هو:
Edward C. Liu, "Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015," Congressional Research Service, June 16, 2011, https://www.fas.org/sgp/crs/intel/R40138.pdf.

(3) صارت القوانين الحالية «مُتقادمة جدا»:
"The President's Radio Address," July 28, 2007, Public Papers of the Presidents of the United States: George W. Bush, 2007, Book II (Washington, D.C.: US Government. Printing Office, 2007), 1027–28, http://www.gpo.gov/fdsys/pkg/PPP-2007-book2/html/PPP-2007-book2-doc-pg1027.htm.

(4) «المراقبة الإلكترونية» لأحد الأمريكيين: نص قانون حماية أمريكا للعام 2007 في:
https://www.govtrack.us/congress/bills/110/s1927/text.

(5) «يربط النقاط بعضها ببعض: على سبيل المثال، انظر:
The 9/11 Commission Report, 408 and passim, http://www.9-11commission.gov/report/911Report.pdf.

(6) «كُومَة القَشّ بكاملها»: الاستعارة استخدمها لأول مرة «ضابط استخبارات سابق» اُقتبستَ في:
Ellen Nakashima and Joby Warrick, "For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All,'" Washington Post, July 14, 2013.
لكن ألكسندر أيضا كان معروفا باستخدام هذه العبارة. (مُقابلات).

(7) مع ذلك، في التاسع من فبراير:
White House press release, Feb. 9, 2009, http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/.

(8) استغرقت المراجعة أكثر من ستين يوما:
White House press release, May 29, 2009, http://www.whitehouse.gov/the-press-office/cybersecurity-event-fact-sheet-and-expected-attendees

(9) على نحو غريب، بدا التقرير مثل:
White House, Cyberspace Policy Review, http://www.whitehouse.gov/as-

sets/documents/Cyberspace_Policy_Review_final.pdf; quotes come from i, iv, v, vi.

(10) «تقاسم المسؤولية»: المصدر نفسه، 17.

(11) «هذا التهديد السيبراني»:

White House, “Remarks by the President on Securing the Nation’s Cyber Infrastructure,” East Room, May 29, 2009.

الفصل الثاني عشر

(1) قام جورج دبليو بوش بنفسه:

David Sanger, Confront and Conceal (New York: Crown, 2012), xii, 190, 200–203.

(2) كانت عملية الألعاب الأولمبية قد بدأت: المصدر نفسه، 191-193

(3) في أثناء الجسّات التي كانت تجريها: المصدر نفسه، 196 وما يليها؛

Kim Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon (New York: Crown, 2014), Ch. 1.

(4) ستكون عملية ضخمة:

Ellen Nakashima and Joby Warrick, “Stuxnet Was Work of U.S. and Israeli Experts, Officials Say,” Washington Post, June 2, 2012.

(5) «مزودات الطاقة غير المنقطعة» uninterruptible power supplies:

Zetter, Countdown to Zero Day, 200201.

(6) برمجِّية خبيثة متعددة الأغراض: المصدر نفسه، 276-279 الكثير من معلومات «زيتر» Zetter مصدرها من المتخصصين في فيروسات الحواسيب في «سيمانتيك» Symantec و«كاسبارسكي لاب» Kaspersky Lab الذين اكتشفوا «ستوكسنت» Stuxnet. عدد أسطر التعليمات البرمجية (الكود) الخبيثة النموذجية يبلغ في المتوسط نحو 175 سطرا. (مقابلات).

(7) للولوج إلى عناصر التحكم (الضوابط): المصدر نفسه، 90، 279.

(8) استغرق الأمر ثمانية أشهر: Sanger, Confront and Conceal, 193.

(9) في الاجتماع التالي: المصدر نفسه، xii.

(10) كان هناك تحد آخر: المصدر نفسه، 194-196؛ ومُقابلات. لم يُكشف بعد عمن ثبَّت ناقلة بيانات (وحدة الذاكرة الفلاشية) المحملة بالبرامج الخبيثة الضارة على الحواسيب الإيرانية. يتكهن البعض أنه عميل إسرائيلي يعمل في نطنز (ناتنز)، والبعض بأنه عميل أجنبي (من المحتمل من مركز عمليات المعلومات التابع لوكالة الاستخبارات المركزية) تسلل إلى المنشأة، ويقول البعض إن ناقلات البيانات (وحدات الذاكرة الفلاشية) الملوثة كانت تنتشر في أنحاء المنطقة إلى أن أدخل شخص إحداها في أحد الحواسيب من دون قصد.

(11) لم تكن البرمجيات الخبيثة: Zetter, Countdown to Zero Day, 61, 117, 123.

(12) حالما وصل أوباما إلى البيت الأبيض: المصدر نفسه، 202.

(13) لكن هذا الفيروس الحاسوبي المتنقل على وجه الخصوص كان مبرمجا: المصدر نفسه، 28.

(14) اتصل أوباما هاتفيا ببوش ليخبره:

In his memoir, Duty (New York: Alfred A. Knopf, 2014), 303,
كتب روبرت غيتس أنه «بعد نحو ثلاثة أسابيع» من تنصيب أوباما، «اتصلت هاتفيا ببوش لأخبره أنه كان لدينا «نجاح كبير في برنامج سري كان هو يهتم به كثيرا». بعد ذلك بفترة وجيزة، «أخبرني أوباما أنه كان سيتصل ببوش ويخبره بشأن النجاح السري». لا يقول غيتس إن البرنامج السري هو «ستوكسنت» Stuxnet، لكن يتضح من السياق أن الأمر كذلك، كما يتضح ذلك من أجزاء أخرى من الكتاب حيث يذكر برنامجا سريا مرتبطا بإيران (190-191) ويستنكر التسريب (328).

(15) في شهر مارس، غيرت وكالة الأمن القومي من نهجها: Zetter, Countdown to Zero Day, 303.

(16) كانت السرعة العادية:

David Albright, Paul Brannan, and Christina Walrond, "ISIS Reports: Stuxnet Malware and Natanz" (Washington, D.C.: Institute for Science and International Security), Feb. 15, 2011, http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf.

(17) كانوا قد عانوا مشكلات تقنية: أشارت نسخة غير سرية من تقدير الاستخبارات القومية لعام 2007 إلى أن إيران كانت تعاني «مشكلات تقنية كبيرة في تشغيل» أجهزة الطرد المركزي («الأحكام الرئيسية من تقييم الاستخبارات القومية حول النشاط النووي الإيراني»، أُعيد نشرها في صحيفة نيويورك تايمز، 4 ديسمبر من العام 2007)؛ كان هذا قبل تفعيل «ستوكسنت» Stuxnet.

(18) مع بداية العام 2010: Zetter, Countdown to Zero Day, 1–3. هناك تقديرات مماثلة في:

Albright et al., "ISIS Reports: Stuxnet Malware and Natanz."

(19) الرئيس أوباما، الذي كان قد أُطلع: في أثناء جلسات الإحاطة بشأن عملية «الألعاب الأولمبية Olympic Games»، انتشرت خرائط مطوية كبيرة لمفاعل نطنز (ناتنز) عبر غرفة العمليات (Sanger, Confront and Conceal, 201).

(20) في آن واحد تقريبا:

Michael Joseph Gross, "A Declaration of Cyber-War," Vanity Fair, February 28, 2011.

لمزيد من التفاصيل، انظر:

Nicholas Falliere, Liam O. Murchu, and Eric Chien, "Symantec Security Response: W32.Stuxnet Dossier," https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; David Kushner, "The Real Story of Stuxnet," IEEE Spectrum, Feb. 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet; Eugene Kaspersky, "The Man Who Found Stuxnet—Sergey Ulasen in the Spotlight," Nota Bene, Nov. 2, 2011, http://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/.

(21) أصدرت شركة «مايكروسوفت» Microsoft تقريرا إرشاديا:

"Microsoft Security Bulletin MS10—046—Critical: Vulnerability in Win-

dows Shell Could Allow Remote Execution," Aug. 2, 2010 (updated Aug. 24, 2010), https://technet.microsoft.com/en-us/library/security/ms10-046.aspx; Zetter, Countdown to Zero Day, 279.

(22) بحلول شهر أغسطس، كانت شركة «سيمانتيك» Symantec قد كشفت:

Nicolas Falliere, "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems," Symantec Security Response Blog, Aug. 6, 2010, http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices.

(23) في سبتمبر، فإن باحثا ألمانيا متخصصا في الأمن:

Sanger, Confront and Conceal, 205–6; Joseph Gross, "A Declaration of Cyber-War."

(24) عند هذه النقطة، أصاب الهلع بعض مخبري البرمجيات الأمريكيين: Zetter, Countdown to Zero Day, 187–89; ومقابلات.

(25) علِم أوباما بالانكشاف في أثناء اجتماع في البيت الأبيض: المصدر نفسه، 357.

(26) أوضح تقييم الموقف:

David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," New York Times, June 1, 2012.

(27) «قدرات هجومية في الفضاء السيبراني:

Quoted in Richard A. Clarke and Robert K. Knake, Cyber War (New York: HarperCollins, 2010), 44–47.

(28) «فريق للهجوم السيبراني»:

Zachary Fryer-Biggs, "U.S. Sharpens Tone on Cyber Attacks from China," DefenseNews, March 18, 2013, http://mobile.defensenews.com/article/303180021;

ومقابلات.

(29) في أثناء العام الأول من فترة رئاسة أوباما:

Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," New York Times, July 18, 2009; Clarke and Knake, Cyber War, 23–30.

(30) خلال فترة العام ونصف العام اللاحقة: Zetter, Countdown to Zero Day, 276-79.

(31) بعد مضي أربعة أشهر:

"Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," New York Times, Oct. 23, 2013.

(32) «أظهروا مقدرة واضحة:

"Iran—Current Topics, Interaction with GCHQ: Director's Talking Points," April 2013, quoted and linked in Glenn Greenwald, "NSA Claims Iran Learned from Western Cyberattacks," The Intercept, Feb. 10, 2015, https://firstlook.org/theintercept/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks/.

الوثيقة مصدرها من تسربات إدوارد سنودِن Edward Snowden تأكدت النقطة الأساسية من خلال مقابلات.

(33) سأل فيها، عند أي نقطة: Gates, Duty, 451; ومقابلات.

(34) «كان للهجمات السيبرانية السابقة تأثير: Sanger, Confront and Conceal, 200.

(35) «مذكرة اتفاق ثلاثية الأطراف: ذُكرت مذكرة الاتفاق في تذييل في:

Barack Obama, Presidential Policy Directive, PPD-20, "U.S. Cyber Operations Policy," Oct. 2012, https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf

التوجيه الرئاسي بشأن العمليات السيبرانية «بي بي دي20- PPD-20». من بين الوثائق التي تسربت بواسطة إدوارد سنودن Edward Snowden.

(36) أحد تقارير العمل بشأن التوجيه: يشار إلى هذا بأقواس معقوفة بارزة (مطبوعة بشكل سميك) في نسخة الوثيقة التي سربها سنودن.

(37) «أنت لا يمكن أن يكون لديك شيء سري:

Andrea Shalal-Esa, "Ex-U.S. General Urges Frank Talk on Cyber Weapons," Reuters, Nov. 6, 2011, http://www.reuters.com/article/2011/11/06/us-cyber-cartwright-idUSTRE7A514C20111106.

(38) «سلطة تطوير:

William B. Black Jr., "Thinking Out Loud About Cyberspace," Cryptolog, Spring 1997 (declassified Oct. 2012), http://cryptome.org/2013/03/cryptolog_135.pdf

كان منصب بلاك في وكالة الأمن القومي - على وجه الدقة - هو مساعدا خاصا لمدير وسائل حرب المعلومات.

الفصل الثالث عشر

(1) «إعادة توازن وضعها العالمي:

Thomas Donilon, speech, Asia Society, New York City, March 11, 2013, http://asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york.

(2) بعد ذلك، في 18 فبراير، نشرت شركة «مانديانت» Mandiant:

Mandiant, APT1: Exposing One of China's Cyber Espionage Units, Feb. 18, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

(3) نشرت صحيفة تايمز Times مقالا طويلا على صفحتها الأولى:

David Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," New York Times, Feb. 18, 2013.

رد الصينيين («غير مسؤول irresponsible»، غير مهني unprofessional، إلخ) مقتبس في المقال نفسه.

(4) في فترة مبكرة تعود إلى العام 2001:

Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," Time, Sept. 5, 2005; Adam Segal, "From Titan Rain to Byzantine Hades: Chinese Cyber Espionage," in Jason Hea-

ley, ed., A Fierce Domain: Conflict in Cyberspace, 1986–2012 (Washington, D.C.: Atlantic Council/Cyber Conflict Studies Association, 2013), 165–93;

ومقابلات.

(5) فقه جديد أطلق عليه اسم «صدام المعلومات»:

Bryan Krekel, Patton Adams, and George Bakos, Occupying the Information High Ground, Prepared for the U.S.-China Economic and Security Review Commission (Northrop Grumman Corporation, March 7, 2012), 9–11. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-066.pdf

(6) وبحلول نهاية العقد: المصدر نفسه، 24-28، 40، 45-46؛ ومقابلات.

(7) كان قد كتب أطروحة عن وسائل حرب المعلومات لنيل درجة الدكتوراه: نشرت على أنها:

Gregory J. Rattray, Strategic Warfare in Cyberspace (Cambridge: MIT Press, 2001);

بقية هذا القسم مصدره من مقابلات..

(8) كانت القرصنة الصينية النمطية تبدأ:

Dmitri Alperovitch, McAfee White Paper, "Revealed: Operation Shady RAT," n.d., http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf; Ellen Nakashima, "Report on 'Operation Shady RAT' Identifies Widespread Cyber-Spying," Washington Post, Aug. 3, 2011; Michael Joseph Gross, "Exclusive: Operation Shady RAT—Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza," Vanity Fair, Sept. 2011; Segal, "From Titan Rain to Byzantine Hades: Chinese Cyber Espionage," 168.

(9) في 6 يونيو، نشرت صحيفتا واشنطن بوست The Washington Post والغارديانThe Guardian اللندنية:

"Verizon Forced to Hand Over Telephone Data—Full Court Ruling," The Guardian, June 5, 2013, accompanying Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," The Guardian, June 6, 2013; "NSA Slides Explain the Prism Data-Collection Program," Washington Post, June 6, 2013, which accompanied Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," Washington Post, June 7, 2013; Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google, and others," The Guardian, June 7, 2013.

كانت صحيفة الغارديان The Guardian وصحيفة البوست Post، اللتان كان لديهما وثائق سنودن، قد دخلتا في منافسة شرسة حول من يستطيع النشر أولا. نُشرت قصة فيريزون لصحيفة الغارديان على الإنترنت في 5 يونيو، ثم ظهرت في نسختها المطبوعة

في 6 يونيو. ثم نُشرت قصة صحيفة البوست على الإنترنت في 6 يونيو، ثم في 7 يونيو في إصدارها المطبوع. للحصول على قائمة بجميع القصص المنشورة عن سنودن في صحيفة بوست، انظر:

http://dewitt.sanford.duke.edu/gellmanarticles/.

(10) تلك كانت هي التقارير الأولى: بالنسبة إلى حسابات الصحافيين بشأن لقاءاتهم مع سنودن، انظر:

"Live Chat: NSA Surveillance: Q&A with Reporter Barton Gellman," July 15, 2014, http://live.washingtonpost.com/nsa-surveillance-bart-gellman.html; and Laura Poitras's documentary film, CitizenFour, 2014

للحصول على آراء منتقدة لسنودن، انظر:

"Fred Kaplan, "Why Snowden Won't (and Shouldn't) Get Clemency," Slate, Jan. 3, 2014, http://www.slate.com/articles/news_and_politics/war_stories/2014/01/edward_snowden_doesn_t_deserve_clemency_the_nsa_leaker_hasn_t_proved_he.html; Mark Hosenball, "NSA Memo Confirms Snowden Scammed Passwords from Colleagues," Reuters, Feb. 13, 2014, http://www.reuters.com/article/2014/02/13/us-usa-security-idUSBREA1C1MR20140213; George Packer, "The Errors of Edward Snowden and Glenn Greenwald," Prospect, May 22, 2014, http://www.prospectmagazine.co.uk/features/the-errors-of-edward-snowden-and-glenn-greenwald.

(11) من تلك النقطة فصاعدا، فإن الرد الصيني السريع القاطع: في قمة لاحقة، في سبتمبر من العام 2015، وافق أوباما وشي على عدم «إجراء أو دعم عن علم» السرقة السيبرانية «للملكية الفكرية» مع «نية توفير ميزة تنافسية للشركات أو القطاعات التجارية». لم تكن الصياغة اللغوية دقيقة: «الدعم عن علم» كانت سيسمح «بالتسامح»، و«نية» العمل كان يمكن إنكارها. على أي حال، فإن الولايات المتحدة لا تفعل هذا النوع من السرقات السيبرانية (هي لا تحتاج إلى أسرار التجارة الصينية)، ولايزال شي (بحماقة وعلى نحو منافٍ للعقل) ينفي تورط الحكومة. ولا تغطي الاتفاقية أشكالا أخرى من الهجمات السيبرانية أو التجسس الإلكتروني، ناهيك عن أن الولايات المتحدة تتورط فيها أيضا. ومع ذلك، أنشأت الصفقة خطا ساخنا وإجراءات للتحقيق في الأنشطة السيبرانية السيئة. ربما تمكن من تعميق التعاون في المستقبل.

White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," Sept. 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

(12) بعد أسبوع واحد من القمة الفاشلة:

Lana Lam and Stephen Chen, "Exclusive: Snowden Reveals More US Cyberspying Details," South China Morning Post, June 22, 2013, http://www.scmp.com/news/hong-kong/article/1266777/exclusive-snowden-safe-hong-kong-more-us-cyberspying-details-revealed?page=all.

(13) سرعان ما جاءت القصص والتقارير الصحافية: لملخص، انظر:

Kaplan, “Why Snowden Won’t (and Shouldn’t) Get Clemency.”

(14) الآن تبعثرت جواهر التاج التي تخص «فورت ميد»:

Jacob Appelbaum, Judith Horchert, and Christian Stocker, “Shopping for Spy Gear: Catalog Advertises NSA Toolbox,” Der Spiegel, Dec. 29, 2013, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

(15) في إطار نظام المراقبة الذي وصفته: هذا النطاق المحتمل للمراقبة، المشمول بثلاث قفزات، شُرح بشكل أوضح في:

Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communication Technologies (White House, Dec. 12, 2013), 103, https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=%22liberty%20and%20security%22%20clarke.

(16) بعد هذا الإفشاء: على سبيل المثال، شهادة الجنرال كيث ألكساندر أمام لجنة مجلس الشيوخ المختارة الدائمة المعنية بالاستخبارات، 18 يونيو من العام 2013.

http://icontherecord.tumblr.com/post/57812486681/hearing-of-the-house-permanent-select-committee-on.

(17) هل تقوم وكالة الأمن القومي بجمع:

Transcribed in Glenn Kessler, “James Clapper’s ‘Least Untruthful’ Statement to the Senate,” http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html.

(18) في اليوم السابق، كان وايدن قد أعطى مكتب كلابر:

Senator Ron Wyden, press release, June 11, 2013, http://www.wyden.senate.gov/news/press-releases/wyden-statement-responding-to-director-clappers-statements-about-collection-on-americans.

(19) أنا ظننت، وإن كان هذا تّأمُّل في الماضي: أندريا ميتشيل Andrea Mitchell، مقابلة مع الجنرال جيمس كلابر James Clapper، قناة «إن بي سي» NBC-TV، 9 يونيو 2013.

(20) تلطيخ لسُمعة:

Steven Burke, “Cisco Senior VP: NSA Revelations Besmirched Reputation of US Companies,” CRN News, Jan. 17, 2014, http://www.crn.com/news/security/240165497/cisco-senior-vp-nsa-revelations-besmirched-reputation-of-us-companies.htm?cid=rssFeed.

(21) كانت ميركل غاضبة ومُستاءة:

Philip Oltermann, “Germany Opens Inquiry into Claims NSA Tapped Angela Merkel’s Phone,” The Guardian, June 4, 2014.

(22) كان في امتعاضها واستشاطتها غضب أكثر من مجرد مَسْحَة:

Anthony Faiola, “Germans, Still Outraged by NSA Spying, Learn Their Country May Have Helped,” Washington Post, May 1, 2015; Reuters,

“Germany Gives Huge Amount of Phone, Text Data to US: Report,” world/europe/12reuters-/12/05/http://www.nytimes.com/reuters/2015 .germany-spying.html

الفصل الرابع عشر

(1) مجموعة رفيعة المستوى:

President Obama, press conference, Aug. 9, 2013, https://www.whitehouse.gov/the-press-Noffice/2013/08/09/remarks-president-press-conference.

(2) في اليوم نفسه:

“Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act,” Aug. 9, 2013, http://www.publicrecordmedia.com/wp-content/uploads/2013/08/EOP2013_pd_001.pdf; “The National Security Agency: Missions, Authorities, Oversight and Partnerships,” Aug. 9, 2013, https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf.

(3) كان صنشتاين قد كتب ورقة بحثية أكاديمية في العام 2008:

Cass R. Sunstein and Adrian Vermeule, “Conspiracy Theories” (Harvard Public Law Working Paper No. 08-03; University of Chicago Public Law Working Paper No. 199), Jan. 15, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1084585.

(4) كان الآخر أيضا من ولاية شيكاغو، وهو جيوفري ستون Geoffrey Stone، انظر بصفة خاصة:

Geoffrey R. Stone, Perilous Times: Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism (New York: W. W. Norton, 2006); Geoffrey Stone, Top Secret: When Our Government Keeps Us in the Dark (New York: Rowman & Littlefield, 2007).

(5) بيتر سواير Peter Swire: peterswire.net؛ ومُقابلات.

(6) إلى أحباء ضحايا:

Transcript, Richard A. Clarke, testimony, 9/11 Commission, March 24, 2004, http://www.cnn.com/TRANSCRIPTS/0403/28/le.00.html.

(7) في إحدى فقرات البرنامج التلفزيوني الإخباري «60 دقيقة» (60 Minutes):

“The CBS 60 Minutes Richard Clarke Interview,” http://able2know.org/topic/20967-1.

(8) نُشر الكتاب في أبريل من العام 2010: للاطلاع على أمثلة انتقادية، انظر:

Ryan Singel, “Richard Clarke’s Cyber War: File Under Fiction,” Wired, April 22, 2010.

(9) الحرب السيبرانية، هذا السيبراني:

Jeff Stein, “Book Review: ‘Cyber War’ by Richard Clarke,” Washington Post, May 23, 2010.

(10) في 27 أغسطس،

http://www.dni.gov/index.php/intelligence-community/review-group

مضمون الاجتماع مصدره من مُقابلات.

(11) صباح اليوم التالي: تاريخ الاجتماع الأول في «فورت ميد» مصدره من الفيديو الترفيهي جدا لجيفري ستون مقدما محاضرة «رحلات» في «جامعة شيكاغو»، في وقت ما في العام 2014،

http://chicagohumanities.org/events/2014/journeys/geoffrey-stone-on-the-

مضمون الدورة مصدره من هذا الفيديو ومن مُقابلات.

(12) كان كلارك في كتابه «الحرب السيبرانية» قد انتقد:

Richard A. Clarke and Robert K. Knake, Cyber War (New York: Harper-Collins, 2010), passim, esp. 44ff.

(13) لم يكن سنودِن يروق له:

“Is Edward Snowden a Hero? A Debate with Journalist Chris Hedges and Law Scholar Geoffrey Stone,” Democracy Now, June 12, 2013, http://www.democracynow.org/2013/6/12/is_edward_snowden_a_hero_a.

ومُقابلات.

(14) علاوة على ذلك، إذا كشفت البيانات الواصفة: إن رقم 22 مسؤولا من وكالة الأمن القومي مصدره من:

White House, Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communication Technologies, Dec. 12, 2013 (hereinafter cited as “President’s Review Group”), 98, https://www.nsa.gov/civil_liberties/_files/liberty_security_prgfinalreport.pdf;

بقية هذا القسم، ما لم يُذكر خلاف ذلك، مصدره من المقابلات.

(15) قفزة ثانية: يمكن العثور على مناقشة واضحة للقفزات في المرجع نفسه، 102 و103.

(16) طوال العام 2012 بكامله: الأعداد 288، 12، 0 مُستشهد بها في المرجع نفسه، 104.

(17) آه، مرحبا؟:

Geoffrey Stone, interview, NBC News, “Information Clearing House,” Dec. 20, 2013, http://www.informationclearinghouse.info/article37174.htm

ومُقابلات.

(18) إنه التسريب المعني بالبرنامج المعروف باسم «بريزم» PRISM: كان هذا أول تسريب للأخبار من سنودن الذي لم يكن قد أعلن بعد أنه المصدر. انظر:

Barton Gellman and Laura Poitras, “U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program,” Washington Post, June 7, 2013,

المناقشة في «فورت ميد» مصدرها من مقابلات.

(19) «الأداة الأبرز»: مُقتبسة في:

Jack Bouboushian, “Feds Ponder Risk in Preserving Spying Data,”

Courthouse News Service, June 6, 2014, http://www.courthousenews.com/2014/06/06/68528.htm.

استخدمت الصياغة اللغوية نفسها لاحقا في بيان وكالة الأمن القومي في 9 أغسطس حول مهامها وسلطاتها (انظر ما ورد آنفا)، وكذلك في بيان مشترك في 22 أغسطس 2013 من قبل وكالة الأمن القومي ومكتب مدير الاستخبارات الوطنية،

http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/917-joint-statement-nsa-and-office-of-the-director-of-national-intelligence.

(20) كان الجنرال ألكسندر قد صرح علنا:

NBC News, June 27, 2013, http://usnews.nbcnews.com/_news/2013/06/27/19175466-nsa-chief-says-surveillance-programs-helped-foil-54-plots;

ومقابلات.

(21) حالما كان هناك احتمال بنسبة 52 في المائة: جرى الاستشهاد بهذا أيضا في:

Gellman and Poitras, “U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program.”

(22) في كل عام، كان يتعين تصديق مُدير الوكالة: President’s Review Group, 138.

(23) «عشرات الآلاف من الاتصالات المحلية الكاملة»: جرى الاستشهاد في المصدر نفسه، 141 و142.

(24) بالنسبة إلى بعض أعضاء اللجنة: مصدر هذا من مُقابلات، لكن الفكرة معبر عنها على مدار التقرير، على سبيل المثال، الصفحات 61، 76، 113 - 116، 125.

(25) استنتج موريل وموظفو اللجنة: المصدر نفسه، 144 و145.

(26) مع ذلك، لم يجدوا في أي من هذه الملفات الثلاثة والخمسين: المصدر نفسه، 104؛ ومقابلات.

(27) أيضا، كشف ألكسندر: المصدر نفسه، 97؛ ومُقابلات.

(28) «هذا هراء»:

Stone, “Journeys” lecture, University of Chicago;

ومقابلات.

(29) «الحد من احتمالات»: President’s Review Group, 118.. وبالنسبة إلى التوصيات الأخرى المذكورة، انظر: 34، 36، 86، 89.

(30) «تخريب، أو تعطيل، أو إضعاف»: المصدر نفسه، 36 و37.

(31) ختاما، وخشية أن يُفسر أي شخص التقرير: كانت هذه هي التوصيات من 37 إلى 46، المصدر نفسه، 39 - 42.

(32) في 13 ديسمبر: المتحدث باسم البيت الأبيض جاي كارني Jay Carney ذكر في إحاطته بتاريخ 16 ديسمبر،

https://www.whitehouse.gov/the-press-office/2013/12/16/daily-briefing-press-secretary-12162013.

(33) «لتعزيز ثقة العامة»: President’s Review Group, 49.

(34) «على الرغم من أن الإفصاحات»: المصدر نفسه، 75 و76.

(35) «أنه لا يوجد دليل على عدم المشروعية»، المصدر نفسه، 76.

(36) «الخطر الكامن»، المصدر نفسه، 113.
(37) «نحن لا نستطيع أن نستبعد»، المصدر نفسه، 114.
(38) في 18 ديسمبر:
White House, President's Schedule, https://www.whitehouse.gov/schedule/president/2013-12-18.
(39) «لا نستطيع منع الهجمات الإرهابية»:
"Remarks by the President on Review of Signals Intelligence," Jan. 17, 2014, https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
(40) «من حيث إنه لا يوجد خط فاصل واضح»:
Liz Gannes, "How Cyber Security Is Like Basketball, According to Barack Obama," re/code, Feb. 14, 2015, http://recode.net/2015/02/14/how-cyber-security-is-like-basketball-according-to-barack-obama/.
(41) الأسئلة التي تُطرَح: كشف عن هذا القرار مايكل دانييل Michael Daniel، رئيس الأمن السيبراني في البيت الأبيض، وحدد هذه المعايير، في مدونته في 28 أبريل 2014، بعنوان:
"Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.
(42) «غير مسبوق وغير مبرر»: الحكم الذي جاء في قضية «الاتحاد الأمريكي للحريات المدنية» American Civil Liberties Union (ACLU) ضد كلابر،
http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf.
حكمت إحدى المحاكم الابتدائية لمصلحة كلابر، ومن ثم أيدت مفهوم محكمة قانون مراقبة الاستخبارات الأجنبية المتعلق بـ «أهمية» وشرعية جمع وكالة الأمن القومي بالجملة؛ محكمة الاستئناف الأمريكية للدائرة الثانية في نيويورك نقضت هذا الحكم وألغته. حللتُ الحكم وتبعاته في:
Fred Kaplan, "Mend It, Don't End It," Slate, May 8, 2015, http://www.slate.com/articles/news_and_politics/war_stories/2015/05/congress_should_revise_the_patriot_act_s_section_215_the_national_security.html
(43) «لكي أكون واضحا»ـ في اليوم نفسه، نشر ستون نسخة مختصرة من حديثه:
Geoffrey R. Stone, "What I Told the NSA," Huffington Post, March 31, 2014, http://www.huffingtonpost.com/geoffrey-r-stone/what-i-told-the-nsa_b_5065447.html;
وتستند هذه الرواية من خطابه إلى ذلك المقال وإلى مُقابلات.

الفصل الخامس عشر

(1) في أولى ساعات الصباح الباكر: معظم مواد اختراق «فيغاس» مصدرها من:
Ben Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hack in Every Server," Bloomberg Businessweek, Dec. 11, 2014, http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-

adelsons-sands-casino-in-las-vegas;

القليل مصدره من مقابلات.

(2) «حراس السلام» Guardians of Peace:

James Cook, "Sony Hackers Have Over 100 Terabytes of Documents," Business Insider, Dec. 16, 2014; Mark Seal, "An Exclusive Look at Sony's Hacking Saga," Vanity Fair, Feb. 2015; Kevin Mandia, quoted in "The Attack on Sony," 60 Minutes, CBS TV, Apr. 12, 2015, http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/.

(3) كانت «سوني» قد اختُرقت قبل ذلك:

Keith Stuart and Charles Arthur, "PlayStation Network Hack," The Guardian, April 27, 2011; Jason Schreier, "Sony Hacked Again: 25 Million Entertainment Users' Info at Risk," Wired.com, May 2, 2011, http://www.wired.com/2011/05/sony-online-entertainment-hack/.

(4) بلغت التكلفة الناشئة عن الأعمال التجارية المفقودة:

Jason Schreier, "Sony Estimates $171 Million Loss from PSN Hack," Wired.com, May 23, 2011, http://www.wired.com/2011/05/sony-psn-hack-losses/.

(5) لذلك، لم تكن الدروس المستفادة في أحد المجالات:

John Gaudiosi, "Why Sony Didn't Learn from Its 2011 Hack," Fortune.com, Dec. 24, 2014, http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

(6) «تُدمِّر بلا رحمة»:

David Tweed, "North Korea to 'Mercilessly' Destroy Makers of Rogen Film," BloombergBusiness, June 26, 2014, http://www.bloomberg.com/news/articles/2014-06-26/north-korea-to-mercilessly-destroy-makers-of-seth-rogan-film.

(7) في العلن، كان المسؤولون الرسميون يقولون:

"The Attack on Sony," 60 Minutes; "NSA Chief Says Sony Attack Traced to North Korea After Software Analysis," Reuters, Feb. 19, 2015, http://www.nytimes.com/reuters/2015/02/19/technology/19reuters-nsa-north-korea-sony.html?_r=0.

(8) كانت مجموعة «دارك سيول» (سيول المعتمة) قد استخدمتها في الماضي:

Brandon Bailey and Youkyung Lee, "Experts Cite Similarities between Sony Hack and 2013 South Korean Hacks," Associated Press, Dec. 4, 2014, http://globalnews.ca/news/1707716/experts-cite-similarities-between-sony-hack-and-2013-south-korean-hacks/.

(9) لكن السبب الحقيقي:

David E. Sanger and Martin Fackler, "NSA Breached North Korean Network before Sony Attack, Officials Say," New York Times, Jan. 18, 2015

ومُقابلات.

(10) «ارتكبت خطأ»:

"Remarks by the President in Year-End Press Conference," White House, Dec. 19, 2014, https://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.

(11) «مجرد هجوم»، بيان الوزير جونسون بشأن الهجوم السيبراني على «سوني بيكتشرز إنترتاينمنت» Sony Pictures Entertainment، وزارة الأمن الداخلي، 19 ديسمبر 2014،

http://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment.

(12) في 22 ديسمبر:

Nicole Perlroth and David E. Sanger, "North Korea Loses Its Link to the Internet," New York Times, Dec. 22, 2014.

أن الحكومة الأمريكية لم تشن الهجوم مصدره من مقابلات.

(13) «الطَلْعَة الأولى من ردنا»، بيان من السكرتير الصحافي بشأن الأمر التنفيذي «فرض عقوبات إضافية فيما يتعلق بكوريا الشمالية»، البيت الأبيض، 2 يناير 2015،

https://www.whitehouse.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-sanctions-respect-north-korea.

القصة وراء الصيغة الحادة مصدرها من مقابلات.

(14) أولئك الذين سمعوا حدة نبرة صوت جيتس: في توجيه الرئيس أوباما بشأن سياسة العمليات السيبرانية الأمريكية «بي بي دي - 20» PPD-20، فإن أحد التوجيهات، التي من الواضح أنها مستوحاة من فكرة جيتس، تنص على ما يلي: بالتنسيق مع وزيري الدفاع والأمن الداخلي، فإن المدعي العام، ومدير الاستخبارات القومية، وغيرهما، وفق ما تقتضي الأمور، سيستمرون في قيادة الجهود للتوصل إلى توافق دولي في الآراء بشأن معايير السلوك في الفضاء السيبراني للحد من احتمال ومنع إجراءات تتخذها دول أخرى من شأنها أن تتطلب من حكومة الولايات المتحدة اللجوء إلى «العمليات الهجومية السيبرانية». في مذكرة لاحقة، تلخص الإجراءات التي كانت الوزارات المعنية قد اتخذتها حتى حينه. الإضافة إلى هذه العبارة تنص: «الإجراء»: [وزارة] الخارجية؛ مستمرو - مما يعني، بعبارة أخرى، لا تقدم: http://fas.org/irp/offdocs/ppd/ppd-20.pdf.

(15) في العام 2014 كانت الأرقام الدقيقة للعام 2014 هي 79.790 انتهاكا، مع 2.122 من المؤكد أنها أدت إلى فقدان البيانات؛ للعام 2013، 63.437 انتهاكا، مع 1.367 خسارة. كان التجسس هو الدافع لـ 18 في المائة من الخروقات؛ كان 27.4 في المائة منها موجها إلى الشركات المصنعة، 20.2 في المائة إلى الدوائر الحكومية.

Verizon, 2014 Data Breach Investigations Report, April 2015, esp. introduction, 32, 52, file:///Users/fred/Downloads/rp_Verizon-DBIR-2014_en_xg%20(3).pdf

لبيانات العام 2013:

Verizon, 2013 Data Breach Investigations Report, April 2014, file:///Users/fred/Downloads/rp_data-breach-investigations-report-2013_en_xg.pdf.

(16) كان قراصنة الحاسوب يمكثون لفترة 205 أيام داخل:

Cybersecurity: The Evolving Nature of Cyber Threats Facing the Private Sector, Before the Subcommittee on Information Technology, 114th Cong. (2015). (Statement of Richard Bejtlich, FireEye Inc.) http://oversight.house.gov/wp-content/uploads/2015/03/3-18-2015-IT-Hearing-on-Cybersecurity-Bejtlich-FireEye.pdf.

(17) في العام 2013، فإن باحثين في الشؤون الأمنية:

Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," Wired, July 21, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

مع ذلك، في وقت سابق صرح فريق من باحثي الجامعة بوجود هذه الثغرة، في:

Stephen Checkoway, et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," http://www.autosec.org/pubs/cars-usenixsec2011.pdf.

تجربة العام 2013 التي أجراها تشارلي ميللر Charlie Miller وزميله كريس فيلاسيك Chris Velasek، صممت لاختبار فرضية تلك الورقة البحثية. قدما ورقة بحثية تتألف من تسع وتسعين صفحة تشرح كيفية اختراقهما (وتوضيح الآثار المزعجة)، في مؤتمر بلاك هات Black Hat الذي عقد في أغسطس من العام 2015 في لاس فيغاس.

"Remote Exploitation of an Unaltered Passenger Vehicle," illmatics.com//remote7.20Car7.20Hacking.pdf.

(18) «لا شيء في هذا الأمر»: الرئيس باراك أوباما، الأمر التنفيذي - تحسين الأمن السيبراني للبنية الأساسية الحرجة، 12 فبراير 2013،

https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

(19) «يُعرقل أو يهزم كلية»:

Department of Defense, Defense Science Board, Task Force Report, Resilient Military Systems and the Advanced Cyber Threat, Jan. 13, 2013, cover memo and executive summary, 1, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

(20) كان بعض أعضاء فريق عمل مجلس علوم الدفاع: المصدر نفسه، الملحق 2؛ «آلة الزمن»، مصدرها من مُقابلات.

(21) «الربط الشبكي»، المصدر نفسه، الملخص التنفيذي، 15.

(22) «أُنشئت على بنى هي أصلا بطبيعتها متقلقلة وغير آمنة»، المصدر نفسه، الغلاف، 1، 31.

(23) «مع القدرات والتكنولوجيا الحالية»، المصدر نفسه.

(24) «حتى ذلك الحين كان الغرض الرئيس»:

Bernard Brodie, the Absolute Weapon (New York: Harcourt Brace, 1946), 73–74, 76.

للمزيد عن برودي، والموضوع بشكل عام، انظر:

Fred Kaplan, the Wizards of Armageddon (New York: Simon &

Schuster, 1983)

(25) «تعريف واستحداث»:

Barack Obama, White House, "The Comprehensive National Cybersecurity Initiative," https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

(26) «استغرق الأمر عدة عقود»:

Department of Defense, Defense Science Board, Task Force Report, Resilient Military Systems and the Advanced Cyber Threat, 51.

في الواقع، في منتصف التسعينيات من القرن العشرين، أجرت مؤسسة «راند» سلسلة من المناورات الحربية التي كانت تحاكي التهديدات والاستجابات في وسائل الحرب السيبرانية، ومعظمها كانت تضم مسؤولي وزارة الدفاع الأمريكية (البنتاغون) من المستوى الأعلى ومساعدي البيت الأبيض كعناصر في المناورة، لكن لم يأخذهم أي من العالمين ببواطن الأمور على محمل الجد. جاءت المناورات مبكرة قليلا جدا ليكون لها تأثير. تم تلخيص المناورات في:

Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, Strategic Information Warfare: A New Face of War (Washington, D.C.: RAND Corporation, 1996).

ندرة التأثير مصدرها من مُقابلات.

(27) النظر في متطلبات:

Undersecretary of Defense (Acquisition, Technology, and Logistics), Memorandum for Chairman, Defense Science Board, "Terms of Reference—Defense Science Board Task Force on Cyber Deterrence," 09-Cyber_-10-Oct. 9, 2014, http://www.acq.osd.mil/dsb/tors/TOR-2014 .Deterrence.pdf

تاريخ الجلسة الأولى وأسماء أعضاء فرقة العمل مصدرها من مقابلات.

(28) في العام 2011، حينما أدرك روبرت غيتس: جرى تلخيص التوجيه، على الرغم من أنه على نحو غير مباشر، في:

Department of Defense, Department of Defense Strategy for Operating in Cyberspace, July 2011, http://www.defense.gov/news/d20110714cyber.pdf; see also Aliya Sternstein, "Military Cyber Strike Teams Will Soon Guard Private Networks," NextGov.com, March 21, 2013, http://www.nextgov.com/cybersecurity/cybersecurity-report/2013/03/military-cyber-strike-teams-will-soon-guard-private-networks/62010/;

ومُقابلات.

(29) «التركيز الأكبر»، مقتبس في:

"Rogers: Cybercom Defending Networks, Nation," DoD News, Aug. 18, 2014, http://www.defense.gov/news/newsarticle.aspx?id=122949.

(30) «بالاشتراك مع الدوائر الحكومية الأخرى»:

Department of Defense, The Department of Defense Cyber Strategy, April 2015; quotes on 5, 14, emphasis added; see also 6, http://www.

defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

أوضحت الوثيقة أن الحكومة لن تكون مسؤولة إلا عن ردع الهجمات السيبرانية التي لها «تداعيات ذات دلالة»، أو ربما الرد عليها، وأضافت، التي «ربما تشتمل على فقدان الأرواح، أو إلحاق ضرر ذي دلالة بالممتلكات، أو عواقب وخيمة خطرة على السياسة الخارجية الأمريكية، أو آثار اقتصادية خطيرة على الولايات المتحدة». بقيت المصطلحات «ذات دلالة» و«خطيرة» غير محددة - سؤال روبرت غيتس، قبل ذلك بتسعة أعوام، عن أي نوع من الهجوم السيبراني يشكل عملا من أعمال الحرب بقي من دون إجابة - لكن البراعة عكست فهما مفاده أن مثل هذه الأسئلة هي سياسية في نهاية المطاف، يحسمها ويبتها القادة السياسيون. كما أن ذلك عكس حقيقة لا مفر منها، وهي أن هذا لم يكن منطقة معتمة فقط، لكن غير مقيدة.

(31) «كيف نحن نُزيد»:

Ellen Nakashima, "Cyber Chief: Efforts to Deter Attacks Against the US Are Not Working," Washington Post, March 19, 2015.

(32) «من المحتمل دولة أو دولتين»:

Patricia Zengerle, "NSA Chief Warns Chinese Cyber Attack Could Shut U.S. Infrastructure," Reuters, Nov. 21, 2014, http://www.reuters.com/article/2014/11/21/usa-security-nsa-idUSL2N0TB0IX20141121.

(33) «الشعب الأمريكي»:

Liberty and Security in a Changing World: President's Review Group, 62.

فرِد كابلان

■ كاتب وصحافي أمريكي متخصص في شؤون الأمن القومي.

■ يكتب عمود «روايات الحرب» (War Stories) في مجلة «سليت» (Slate) الأمريكية، وهو حاصل على جائزة «بوليتزر» عن مقال نشرته صحيفة «بوسطن غلوب».

■ ألَّف أربعة كتب سابقة، هي:

1 - «المتمردون: ديفيد بترايوس ومؤامرة تغيير الطريقة الأمريكية للحرب» The Insurgents: David Petraeus and the Plot to Change the American Way of War (الذي كان ضمن القائمة النهائية لجائزة «بوليتزر»).

2 - «1959: العام الذي تغير فيه كل شيء» 1959: The Year Everything Changed.

3 - «المؤمنون بأحلام اليقظة: كيف دمرت بضع أفكار كبرى القوة الأمريكية» Daydream Believers: How a Few Grand Ideas Wrecked American Power.

4 - «سحرة هرمجدون» The Wizards of Armageddon (الذي حصل على جائزة كتاب العام في مسابقة واشنطن للكتاب السياسي الشهري).

■ حصل على درجة البكالوريوس من كلية أوبرلين Oberlin College في ولاية أوهايو، ودرجتي الماجستير والدكتوراه في العلوم السياسية من معهد ماساتشوستس للتكنولوجيا Massachusetts Institute of Technology (MIT).

■ يعيش في بروكلين مع زوجته بروك غلادستون.

د. لؤي عبدالمجيد السيد

■ باحث أول ومساعد عميد مركز البحوث والاستشارات لقطاع النقل البحري - الإسكندرية - جمهورية مصر العربية.

■ حاصل على دكتوراه الفلسفة في الحوسبة - كلية العلوم والتكنولوجيا - جامعة بليموث - المملكة المتحدة.

■ حاصل على ماجستير تكنولوجيا المعلومات - معهد الدراسات العليا والبحوث - جامعة الإسكندرية - جمهورية مصر العربية.

■ حاصل على دبلوم الدراسات العليا في تكنولوجيا المعلومات ودبلوم الدراسات البيئية في ترشيد الطاقة من معهد الدراسات العليا والبحوث – جامعة الإسكندرية.

■ حاصل على بكالوريوس العلوم - جامعة الإسكندرية.

■ له عدد من الأبحاث العلمية المنشورة في مؤتمرات ومجلات علمية.

■ أدار وشارك في العديد من مشروعات تطبيق تكنولوجيا المعلومات في صناعة النقل البحري في كل من مصر والسودان وسورية.

■ أحد رواد نشر وتطبيق نظام تبادل البيانات إلكترونيا (Electronic Data Interchange – EDI) في قطاع النقل البحري المصري.

■ عضو نقابة المهن العلمية بجمهورية مصر العربية، وعضو جمعية نظم المعلومات – أطلنطا – الولايات المتحدة الأمريكية.

■ مستشار ومتخصص في نمذجة وإعادة هندسة العمليات الإدارية، وتطوير نظم المعلومات المتكاملة لمجتمع الميناء، ونمذجة وبناء نظم المعلومات متعددة الوكلاء Multi-agent Systems.

■ تأتي الترجمة والتعريب في صدارة اهتماماته لإثراء المكتبة العربية بالكتب العلمية، خصوصا في مجال تكنولوجيا المعلومات وتطبيقاتها الحديثة، والتي تفتقر إليها المكتبة العربية.

■ ترجم لسلسلة «عالم المعرفة» كتاب «الثورة الرابعة.. كيف يعيد الغلاف المعلوماتي تشكيل الواقع الإنساني» The Fourth Revolution.. How the Infosphere is Reshaping Human Reality، (العدد 452) تأليف البروفيسور لوتشيانو فلوريدي، واختير هذا الكتاب ضمن القائمة القصيرة للكتب المرشحة لنيل جائزة الشيخ زايد الدولية للكتاب في فرع الترجمة في دورتها الثانية عشرة في العام 2017 - 2018.

سلسلة عالم المعرفة

«عالم المعرفة» سلسلة كتب ثقافية تصدر في مطلع كل شهر ميلادي عن المجلس الوطني للثقافة والفنون والآداب - دولة الكويت - وقد صدر العدد الأول منها في شهر يناير من العام 1978.

تهدف هذه السلسلة إلى تزويد القارئ بمادة جيدة من الثقافة تغطي جميع فروع المعرفة، وكذلك ربطه بأحدث التيارات الفكرية والثقافية المعاصرة. ومن الموضوعات التي تعالجها تأليفا وترجمة:

1 - الدراسات الإنسانية: تاريخ ـ فلسفة - أدب الرحلات - الدراسات الحضارية - تاريخ الأفكار.

2 - العلوم الاجتماعية: اجتماع - اقتصاد - سياسة - علم نفس - جغرافيا - تخطيط - دراسات استراتيجية - مستقبليات.

3 - الدراسات الأدبية واللغوية: الأدب العربي - الآداب العالمية - علم اللغة.

4 - الدراسات الفنية: علم الجمال وفلسفة الفن - المسرح - الموسيقى - الفنون التشكيلية والفنون الشعبية.

5 - الدراسات العلمية: تاريخ العلم وفلسفته، تبسيط العلوم الطبيعية (فيزياء، كيمياء، علم الحياة، فلك) ـ الرياضيات التطبيقية (مع الاهتمام بالجوانب الإنسانية لهذه العلوم)، والدراسات التكنولوجية.

أما بالنسبة إلى نشر الأعمال الإبداعية ـ المترجمة أو المؤلفة ـ من شعر وقصة ومسرحية، وكذلك الأعمال المتعلقة بشخصية واحدة بعينها فهذا أمر غير وارد في الوقت الحالي.

وتحرص سلسلة «عالم المعرفة» على أن تكون الأعمال المترجمة حديثة النشر.

وترحب السلسلة باقتراحات التأليف والترجمة المقدمة من المتخصصين، على ألا يزيد حجمها على 350 صفحة من القطع المتوسط، وأن تكون مصحوبة بنبذة وافية عن الكتاب وموضوعاته وأهميته ومدى جدته وفي حالة الترجمة ترسل نسخة مصورة من الكتاب بلغته الأصلية كما ترفق مذكرة بالفكرة العامة للكتاب، وكذلك يجب أن تدوّن أرقام صفحات الكتاب الأصلي المقابلة للنص المترجم على جانب الصفحة المترجمة، والسلسلة لا يمكنها النظر في أي ترجمة ما لم تكن مستوفية لهذا الشرط. والمجلس غير ملزم بإعادة المخطوطات والكتب الأجنبية في حالة الاعتذار عن عدم نشره. وفي جميع الحالات ينبغي إرفاق سيرة ذاتية لمقترح الكتاب تتضمن البيانات الرئيسية عن نشاطه العلمي السابق.

وفي حال الموافقة والتعاقد على الموضوع ــ المؤلف أو المترجم ــ تصرف مكافأة للمؤلف مقدارها ألفا دينار كويتي، وللمترجم مكافأة بمعدل ثلاثين فلسا عن الكلمة الواحدة في النص الأجنبي (وبحد أقصى مقداره ألفان وخمسمائة دينار كويتي).

سعر النسخة

الكويت ودول الخليج	دينار كويتي
الدول العربية	ما يعادل دولارا أمريكيا
خارج الوطن العربي	أربعة دولارات أمريكية

الاشتراكات

دولة الكويت

للأفراد	15 د. ك
للمؤسسات	25 د. ك

دول الخليج

للأفراد	17 د. ك
للمؤسسات	30 د. ك

الدول العربية

للأفراد	25 دولارا أمريكيا
للمؤسسات	50 دولارا أمريكيا

خارج الوطن العربي

للأفراد	50 دولارا أمريكيا
للمؤسسات	100 دولار أمريكي

تسدد الاشتراكات والمبيعات مقدما نقدا أو بشيك باسم المجلس الوطني للثقافة والفنون والآداب، مع مراعاة سداد عمولة البنك المحول عليه المبلغ في الكويت، ويرسل إلينا بالبريد المسجل على العنوان التالي:

المجلس الوطني للثقافة والفنون والآداب

ص. ب 23996 الصفاة - الرمزي البريدي 13100

دولة الكويت

بدالة: 22416006 (00965)

داخلي: 1196/ 1195/ 1194/ 1153/1193/ 1152

أسماء وأرقام وكلاء التوزيع

أولاً: التوزيع المحلي – دولة الكويت

م	الدولة	وكيل التوزيع	رقم الهاتف	رقم الفاكس	الإيميل
1	الكويت	المجموعة الإعلامية العالمية	00965 24826820 /1/2	2482682300965 /	im_grp50@yahoo.com
ثانياً: التوزيع الخارجي					
2	السعودية	الشركة السعودية للتوزيع	00966114871414	121277400966 /12121766 –	bander.shareef@saudidistribution.com babiker.khalil@saudidistribution.com
3	البحرين	مؤسسة الأيام للنشر	3661616800973 /17617733 –	1761774400973 /	cir@alayam.com rudainaa.ahmed@alayam.com
4	الإمارات	شركة الإمارات للطباعة والنشر والتوزيع	00971 43916501 /2/3	4391801900971 /43918354 –	eppdc@emirates.net.ae info@eppdco.com essam.ali@eppdco.com
5	سلطنة عُمان	مؤسسة العطاء للتوزيع	2449139900968 /24492936 – 24496748 –	2449320000968 /	alattadist@yahoo.com
6	قطر	شركة دار الثقافة	4462218200974 /44621942 –	4462180000974 /	thaqafadist@qatar.net.qa
7	مصر	مؤسسة أخبار اليوم	00202 25782700/1/2/3/4/5 00202 25806400	2578254000202 /	ahmed_isaac2008@hotmail.com
8	لبنان	مؤسسة نعنوع الصحفية للتوزيع	00961 1666314 /15	165325900961 / 165326000961 /	topspeed1@hotmail.com
9	تونس	الشركة التونسية	7132249900216 /	7132300400216 /	sotupress@sotup.com.nt
10	المغرب	الشركة العربية الأفريقية	52224920000212 /	52224921400212 /	s.wardi@sapress.ma
11	الأردن	وكالة التوزيع الأردنية	79720409500962 /6535885 –	6533773300962 /	alshafiei.ankousha@aramex.com basem.abuhameds@aramex.com
12	فلسطين	شركة رام الله للتوزيع والنشر	2298080000970 /	2296413300970 /	wael.kassess@rdp.ps
13	اليمن	القائد للنشر والتوزيع	124088300967 /	124088300967 /	alkaidpd@yahoo.com
14	السودان	دار الريان للثقافة والنشر والتوزيع	83242702002491 /	83242703002491 /	daralryan_cup22@hotmail.com daralryan_12@hotmail.com

اتحاد الموزعين العرب
ARAB DISTRIBUTORS UNION

تنويــــه

للاطـلاع علـى قائمـة كتـب السلسـلة انظـر عدد ديسـمبر (كانـون الأول) مـن كل سـنة، حيـث توجد قائمة كاملة بأسماء الكتب المنشورة في السلسلة منذ يناير 1978.

يمكنكم الاشتراك والحصول على نسختكم الورقية من إصدارات المجلس الوطني للثقافة والفنون والآداب من خلال الدخول إلى موقعنا الإلكتروني:

https://www.nccal.gov.kw/#CouncilPublications

البيان	عالم المعرفة		الثقافة العالمية		عالم الفكر		إبداعات عالمية		جريدة الفنون		المسرح العالمي	
	د.ك	دولار	د.ك	دولار	د.ك	دولار	د.ك	دولار	د.ك	دولار	د.ك	دولار
مؤسسة داخل الكويت	25		12		12		20		12		20	
أفراد داخل الكويت	15		6		6		10		8		10	
مؤسسات دول الخليج العربي	30		16		16		24			36	24	
أفراد دول الخليج العربي	17		8		8		12			24	12	
مؤسسات خارج الوطن العربي		100		50		40		100		48		100
أفراد خارج الوطن العربي		50		25		20		50		36		50
مؤسسات في الوطن العربي		50		30		20		50		36		50
أفراد في الوطن العربي		25		15		10		25		24		25

قسيمة اشتراك في إصدارات
المجلس الوطني للثقافة والفنون والآداب

الرجاء ملء البيانات في حالة رغبتكم في: تسجيل اشتراك ☐ تجديد اشتراك ☐

الاسم:	
العنوان:	
المدينة:	الرمز البريدي:
البلد:	
رقم الهاتف:	
البريد الإلكتروني:	
اسم المطبوعة:	مدة الاشتراك:
المبلغ المرسل:	نقدا / شيك رقم:
التوقيع:	التاريخ: / / 20م

المجلس الوطني للثقافة والفنون والآداب - إدارة النشر والتوزيع - مراقبة التوزيع

ص.ب: 23996 - الصفاة - الرمز البريدي 13100

دولة الكويت


المجلس الوطني
للثقافة والفنون والآداب



هذا الكتاب...

مع هيمنة الهجمات السيبرانية على أخبار الصفحات الأولى، وانضمام قراصنة الحاسـوب إلى قائمة التهديدات العالمية، وتحذير كبار الجنرالات من الحرب السيبرانية المقبلة، يقدم الكاتب الصحافي فرِد كابلان - الحائز جائزة «بوليتزر» - في كتابه «المنطقة المعتمة.. التاريخ السري للحرب السيبرانية» تاريخا تنويريا مناسبا.

يسبر كابلان الأروقة الداخلية لوكالة الأمن القومي، والوحدات فائقة السرية في وزارة الدفاع الأمريكية (البنتاغون)، وفرق «وسائل حرب المعلومات» في الأفرع العسكرية، والمساجلات السياسية في البيت الأبيض، من أجل سرد هذه القصة - التي لم تُذكر من قبل - عن الضباط والمسؤولين والعلماء والجواسيس الذين استنبطوا هذا النمط الجديد من الحرب، والذين كانوا يُخططون لهذه الحروب طوال عقود، وفي كثير من الأحيان كان الناس يعرفون أن هؤلاء هم الذين يشنونها.

إنها قصة تمتد عبر نصف قرن، منذ اختراع الإنترنت - حينما حذر أحد رواد مجال الحاسبات من أن شبكات المعلومات تخلق نقاط ضعف وثغرات أمنية جديدة للجيش والمجتمع - إلى عناوين الأخبار اليوم. منذ التوجيه الرئاسي الذي لا يُعرف عنه سوى القليل، والذي وقعه الرئيس رونالد ريغان (التوجيه الذي أطلق العنان لمعركة مازالت قائمة بين الأمن والخصوصية)، إلى الرشقات الافتتاحية في حرب الخليج في العام 1991 (إذ أدت السيبرانية دورا لم يُعلن عنه من قبل)، إلى الأبعاد السيبرانية للصراعات في هاييتي، وصربيا، وسورية، وجمهوريات الاتحاد السوفييتي السابق، والعراق، وإيران؛ يروي كتاب «المنطقة المعتمة» تفاصيل مذهلة عن ماضٍ غير معروف يُشع على مستقبلنا ضوءا مُثيرا للقلق.

المنطقة المعتمة

تأليف: فرِدْ كابلان
ترجمة: لؤي عبدالمجيد

ISBN 978 - 99906 - 0 - 627 - 0

470
مارس
2019



إصدارات المجلس متوافرة إلكترونيا على موقعنا:
WWW.NCCAL.GOV.KW/PUBLICATIONS